

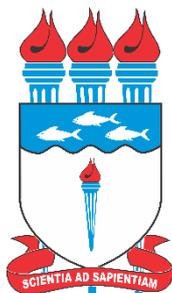
UNIVERSIDADE FEDERAL DE ALAGOAS – UFAL
CAMPUS ARAPIRACA – UNIDADE EDUCACIONAL DE PENEDO
CURSOS DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

GABRIEL ROBERTO RODRIGUES

**INVESTIGANDO O USO DA TECNOLOGIA BLOCKCHAIN NO SETOR DA SAÚDE:
UMA ANÁLISE DO ESTADO DA ARTE E DA PRÁTICA**

PENEDO

2022



UNIVERSIDADE FEDERAL DE ALAGOAS – UFAL
CAMPUS ARAPIRACA – UNIDADE EDUCACIONAL DE PENEDO
CURSOS DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

GABRIEL ROBERTO RODRIGUES

**INVESTIGANDO O USO DA TECNOLOGIA BLOCKCHAIN NO SETOR DA SAÚDE:
UMA ANÁLISE DO ESTADO DA ARTE E DA PRÁTICA**

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação na Universidade Federal de Alagoas – Unidade Educacional de Penedo.

Orientador: Prof. Dr. André Magno Costa de Araújo

PENEDO

2022



Universidade Federal de Alagoas – UFAL
Campus Arapiraca
Unidade Educacional Penedo
Biblioteca Setorial Penedo-BSP

R696i Rodrigues, Gabriel Roberto
Investigando o uso da tecnologia Blockchain no setor da saúde: uma análise do estado da arte e da prática / Gabriel Roberto Rodrigues. – Penedo, AL, 2022. 60 f.: il.

Orientador(a): Prof. Dr. André Magno Costa de Araújo.
Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Universidade Federal de Alagoas, *Campus* Arapiraca, Unidade Educacional Penedo, Penedo, AL, 2022.
Disponível em: Universidade Digital (UD) – UFAL (*Campus* Arapiraca).
Referências: f. 56-60.

1. Blockchain. 2. Registro Eletrônico – Saúde. 3. Sistemas de Informações – Saúde. I. Araújo, André Magno Costa de. II. Título.

CDU 004

Bibliotecária responsável: Eliúde Maria da Silva
CRB - 4 / 1834

Gabriel Roberto Rodrigues

INVESTIGANDO O USO DA TECNOLOGIA BLOCKCHAIN NO SETOR DA SAÚDE: UMA
ANÁLISE DO ESTADO DA ARTE E DA PRÁTICA.

Monografia apresentada como requisito parcial
para obtenção do grau de Bacharel em Sistemas
de Informação na Universidade Federal de Alagoas
– Unidade Educacional de Penedo.

Data de Aprovação: 03/ 03/ 2021

Banca Examinadora

Prof. Dr. André Magno Costa de Araújo
Universidade Federal de Alagoas – UFAL
Campus Arapiraca – Unidade Educacional de Penedo
Orientador

Prof. Dr. Davy de Medeiros Baía
Universidade Federal de Alagoas – UFAL
Campus Arapiraca – Unidade Educacional de Penedo
Examinador

Prof. Me. André Almeida Silva
Universidade Federal de Alagoas – UFAL
Campus Arapiraca – Unidade Educacional de Penedo
Examinador

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a Deus, pela oportunidade e as condições que me foram concebidas, que me direcionaram a estar no presente momento, bem como a saúde e disposição para sempre seguir em frente.

Agradeço a minha mãe, Eliane Roberto, por sempre estar ao meu lado, apoiando nos diversos momentos e me ajudando a alcançar meus sonhos.

Agradeço a todos os professores que contribuíram com essa jornada e a busca do sonho, especialmente ao professor e orientador André Magno Costa de Araújo, pelos ensinamentos e conselhos, bem como pela oportunidade de contribuir com a universidade.

Agradeço a um grande amigo, João Tadashy Nakamura Yukimaru pelo apoio em diversos momentos e os conselhos que me ajudaram a evoluir pessoalmente e profissionalmente.

Agradeço aos meus amigos, Rendrikson de Oliveira Soares, Matheus de Melo Surica, José Vitor de Abreu Silva, José dos Santos Neto e Henrique de Couto Melo pelo apoio e amizade durante essa jornada acadêmica.

E por fim, agradeço a todos os que contribuíram de alguma forma durante todo esse período.

RESUMO

Com a evolução dos sistemas de informações na sociedade, diversos setores foram beneficiados com as soluções tecnológicas, são propostas que evoluem, trazendo mais eficiência para os processos em que são necessárias. A área da saúde também se beneficiou com tais inovações e, com o advento dos registros eletrônicos de saúde, várias possibilidades foram alcançadas, no tocante a velocidade no armazenamento e processamento dos dados, bem como no compartilhamento entre entidades de saúde. A redução de custos e o aumento da eficiência é uma busca contínua de qualquer organização, isso fomenta o surgimento de novas tecnologias que se propõem a resolver problemas atuais. A Blockchain é uma tecnologia emergente que possibilita diversos tipos de soluções que podem beneficiar o setor da saúde, garantindo eficiência em diversos processos. Este trabalho tem como objetivo investigar como a tecnologia Blockchain tem sido utilizada no setor de saúde para garantir a imutabilidade e o acesso permissionado aos dados do paciente. Para isso, serão investigados no estado da arte e da prática, pesquisas que abordam o desenvolvimento e a validação de soluções computacionais com as seguintes áreas: Técnicas de armazenamento, plataformas de desenvolvimento e padrões de interoperabilidade de dados clínicos dos pacientes, ao final serão apontados os principais avanços identificados no setor.

Palavras-chaves: Blockchain, Registros Eletrônicos de Saúde, Sistemas de Informações em Saúde.

ABSTRACT

With the evolution of information systems in society, several sectors have benefited from technological solutions, proposals that evolve, bringing more efficiency to the processes in which they are needed. The health area also benefited from such innovations and, with the advent of electronic health records, several possibilities were achieved, regarding the speed in data storage and processing, as well as in the sharing between health entities. Reducing costs and increasing efficiency is a continuous search for any organization, this encourages the emergence of new technologies that propose to solve current problems. Blockchain is an emerging technology that enables different types of solutions that can benefit the health sector, ensuring efficiency in various processes. This work aims to investigate how Blockchain technology has been used in the health sector to ensure immutability and permissioned access to patient data. For this, state of the art and practice will be investigated, researches that address the development and validation of computational solutions with the following areas: Storage techniques, development platforms and interoperability standards of clinical data of patients, at the end will be pointed out the main advances identified in the sector.

Keywords: Blockchain, Electronic Health Records, Information Systems in Healthcare.

LISTA DE FIGURAS

Figura 1 – Funcionamento de uma Blockchain	15
Figura 2 – Organização dos blocos em uma Blockchain	16
Figura 3 – Componentes do bloco	17
Figura 4 – Esquema centralizado de transações	18
Figura 5 – Funcionamento básico de um Smart Contract na nuvem	20
Figura 6 – Processos do Smart Contract	21
Figura 7 – Esquema de uma rede de livro-razão distribuída	23
Figura 8 – Critérios da pesquisa esquematizado	27
Figura 9 – Trabalhos do Estado da Arte	28
Figura 10 – Trabalhos do Estado da Prática	33
Figura 11 – Classificações dos trabalhos	50
Figura 12 – Classificação dos temas principais de cada trabalho	52

LISTA DE TABELAS

Tabela 1 – Classificação dos Trabalhos	48
---	-----------

SUMÁRIO

1.	INTRODUÇÃO	9
1.1.	Contextualização e Motivação	9
1.2.	Objetivos	10
1.2.1.	Objetivos Gerais	10
1.2.2.	Objetivos Específicos	11
1.3.	Metodologia	11
1.4.	Organização do Trabalho	12
2.	REFERENCIAL TEÓRICO	13
2.1.	Fundamentos da Blockchain	13
2.2.	Tecnologias Blockchain	17
2.2.1.	Blockchain 1.0	18
2.2.2.	Blockchain 2.0	18
2.2.2.1.	Livro Razão Distribuído	21
2.2.3.	Blockchain 3.0	22
3.	ANÁLISE DO USO DA TECNOLOGIA BLOCKCHAIN NO SETOR DE SAÚDE	25
3.1.	Critérios Adotados na Pesquisa	25
3.2.	Análise do Estado da Arte	26
3.3.	Análise do Estado da Prática	31
4.	RESULTADOS E DISCUSSÕES	47
4.1.	Oportunidades e Desafios no Estado da Arte	52
4.2.	Oportunidades e Desafios no Estado da Prática	53
5.	CONCLUSÃO	55
5.1.	Considerações Finais	55
5.2.	Trabalhos Futuros	55
	REFERÊNCIAS	56

1. INTRODUÇÃO

O seguinte trabalho se propõe a realizar uma investigação do estado da arte e da prática do uso da tecnologia Blockchain na área da saúde, apresentando conceitos fundamentais que cercam a temática, propostas de trabalhos que vêm sendo realizados e analisando como o uso de tal tecnologia pode contribuir de forma positiva para o setor. Este capítulo está organizado da seguinte maneira: Na Seção 1.1 é apresentada a contextualização e a motivação para a realização dessa pesquisa. Na Seção 1.2 serão apresentados os objetivos, sendo 1.2.1 Objetivos Gerais e 1.2.2 Objetivos Específicos. Na Seção 1.3 será discutida a metodologia utilizada na elaboração do trabalho, e por fim, na Seção 1.4 será apresentada a organização dos demais capítulos deste documento.

1.1. CONTEXTUALIZAÇÃO E MOTIVAÇÃO

É indiscutível a evolução proporcionada pela Tecnologia da Informação nos mais diversos setores da sociedade, e nesse sentido, a área da saúde é uma das que vem sendo beneficiada por esse avanço tecnológico. Os registros médicos antes da era digital eram armazenados em papel, o que tornava diversos processos mais rudimentares e dificultava questões como agilidade no registro e na busca dos dados, bem como no compartilhamento adequado das informações. Com o advento dos Sistemas de Informação, criou-se a possibilidade dos Registros Eletrônicos de Saúde (RES), uma maneira de armazenar e compartilhar os registros de uma forma mais ampla e eficiente.

De acordo com Spínola, M. Pessôa, M., (1997) a informação trata-se de um recurso poderoso para uma organização pois, através dela, pode-se ter o domínio dos diversos parâmetros que regem sua dinâmica. Nos sistemas empresariais, a informação é reconhecida como o recurso mais importante para a tomada de decisões, sendo necessário que haja uma malha de informações, abrangendo diversos aspectos técnicos-científicos, administrativos, mercadológicos, econômicos, legais, ambientais e políticos.

A busca por soluções que utilizem essas informações para processos de interesse é crescente e, na área da saúde, o uso da tecnologia da informação é utilizado como uma ferramenta para o gerenciamento da informação e isso é um componente essencial no processo de prestação de serviços aos pacientes.

No entanto, existem alguns problemas que envolvem a área, como a interoperabilidade entre os sistemas, ou seja, a capacidade de comunicação entre os

diversos sistemas existentes. O armazenamento de dados e a troca de informações, que devem estar disponíveis para as diferentes organizações, bem como médicos e institutos de pesquisas, e como garantir que tais procedimentos ocorram de forma segura e econômica? Com isso, vem a necessidade de tecnologias que tornem os sistemas de informação cada vez mais eficientes e seguros.

A utilização da tecnologia Blockchain vem se tornando alvo de discussões nos últimos anos como uma forma eficaz de resolver tais problemas, em diversas implementações no setor da saúde. A tecnologia Blockchain redefine a gestão de dados e o processamento, devido a sua capacidade de adaptabilidade e segmentação como nunca houve antes. Essa evolução tecnológica proporcionou avanços nos sistemas de informação de saúde, aperfeiçoamentos em áreas como o armazenamento de dados e computação em nuvem, proteção e privacidade de dados do paciente e a possibilidade de o paciente acessar e compartilhar seus dados de forma segura.

A garantia dessa segurança é importante para qualquer organização de saúde, aplicações baseadas em Blockchain podem resolver diversos desses problemas. Segundo Conceição, A.F. et al. (2019) a tecnologia Blockchain pode ser utilizada no controle de acesso dos dados e na distribuição de informações sensíveis, também para garantir transparência e auditabilidade de prestação de serviços, na interoperabilidade de dados entre outras situações.

Dessa forma, tendo em vista o contexto apresentado, o seguinte trabalho possui como principal motivação, a oportunidade de contribuir com o setor de saúde, investigando como a tecnologia Blockchain tem sido utilizada nas áreas de armazenamento de dados, plataformas de desenvolvimento e padrões de interoperabilidade. Ao final desta investigação, pretende-se mostrar os principais avanços identificados e materializar as principais oportunidades de pesquisa mapeadas do estado da arte e da prática.

1.2. OBJETIVOS

A seguir serão apresentados os objetivos gerais e específicos do presente trabalho.

1.2.1. OBJETIVOS GERAIS

Este trabalho tem como objetivo investigar como a tecnologia Blockchain tem sido utilizada no setor da saúde para garantir imutabilidade e o acesso permissionado aos dados do paciente, bem como novas perspectivas e tendências do uso da Blockchain no setor.

Para isso, serão investigados no estado da arte e da prática pesquisas que abordam o desenvolvimento e a validação de soluções computacionais com as seguintes áreas: Técnicas de armazenamento, plataformas de desenvolvimento e padrões de interoperabilidade de dados clínicos dos pacientes. Ao final desse estudo, serão apontados os principais avanços identificados.

1.2.2. OBJETIVOS ESPECÍFICOS

A seguir serão listados os objetivos específicos do trabalho:

- Entender como o Blockchain funciona, abrangendo seu funcionamento;
- Analisar os contratos inteligentes e seu funcionamento;
- Investigar como a tecnologia Blockchain pode beneficiar o setor da saúde e quais trabalhos vêm sendo realizados nesse sentido, tendo em vista as áreas citadas anteriormente;
- Realizar um mapeamento dos trabalhos que vêm sendo realizados, classificando-os de acordo com a temática abordada;
- Propor oportunidades e tendências de pesquisa a partir dos resultados analisados.

1.3. METODOLOGIA

Tendo em vista as necessidades da área, o seguinte trabalho utilizará uma metodologia descritiva e exploratória, assim como uma análise bibliográfica. Com o objetivo de compreender o domínio do problema atual e como a tecnologia pode melhorar o setor, identificando também as soluções que vêm sendo discutidas e trabalhadas.

Por meio da revisão bibliográfica, serão identificados no estado da arte e da prática as pesquisas e implementações que abordam a utilização da tecnologia Blockchain nas áreas de armazenamento, desenvolvimento de aplicações e padrões de interoperabilidade de dados.

Vale ressaltar que, para o estado da arte foram considerados os trabalhos que realizam uma revisão teórica, porém não propõem soluções computacionais e validação das mesmas. Para o estado da prática foram selecionados trabalhos que propõem tais soluções.

1.4. ORGANIZAÇÃO DO TRABALHO

A partir da Seção 2 será apresentado o Referencial Teórico, sendo a Seção 2.1 os Fundamentos da Blockchain, apresentando conceitos fundamentais sobre os Registros Eletrônicos de Saúde e a tecnologia Blockchain. Na Seção 2.2 serão discutidas as Tecnologias Blockchain, apresentando tecnologias que foram originadas deste importante conceito. Na Seção 3 é apresentada a revisão sistemática, sendo a Seção 3.1 a análise do estado da arte, enquanto a Seção 3.2 aborda a análise do estado da prática. A partir da Seção 4 serão demonstrados os resultados e discussões, seguido por 4.1 as oportunidades e desafios no estado da arte e 4.2 as oportunidades e desafios no estado da prática. Por fim, na Seção 5 serão feitas as considerações finais e indicações de trabalhos futuros.

2. REFERENCIAL TEÓRICO

A seguir será apresentado o referencial teórico deste trabalho, contendo os conceitos fundamentais que cercam a temática.

2.1. FUNDAMENTOS DA BLOCKCHAIN

A utilização de tecnologias nas mais diversas áreas do desenvolvimento social vêm sendo algo natural nos dias de hoje, a Tecnologia da Informação (TI) influencia todos os setores do mercado, da indústria e dos serviços. A área da saúde é um dos setores que mais vem se beneficiando com o auxílio da Tecnologia da Informação, tornando os vários processos cada vez mais eficientes. Segundo Pinochet (2011), a sociedade começou a presenciar o advento dos registros eletrônicos de saúde em diversos países.

Além disso, os Sistemas de Informação estão sendo amplamente adotados no apoio à saúde da população e nas atividades de saúde pública relacionados à prevenção e promoção de saúde, controle de doenças, vigilância e monitoramento. Tanto na área pública, ou privada, em ambos os setores é nítida a importância do investimento em novas tecnologias que sejam capazes de aumentar sua eficiência e melhorar a qualidade dos serviços. Uma tecnologia recente vem ganhando atenção por suas propostas e soluções, a Blockchain.

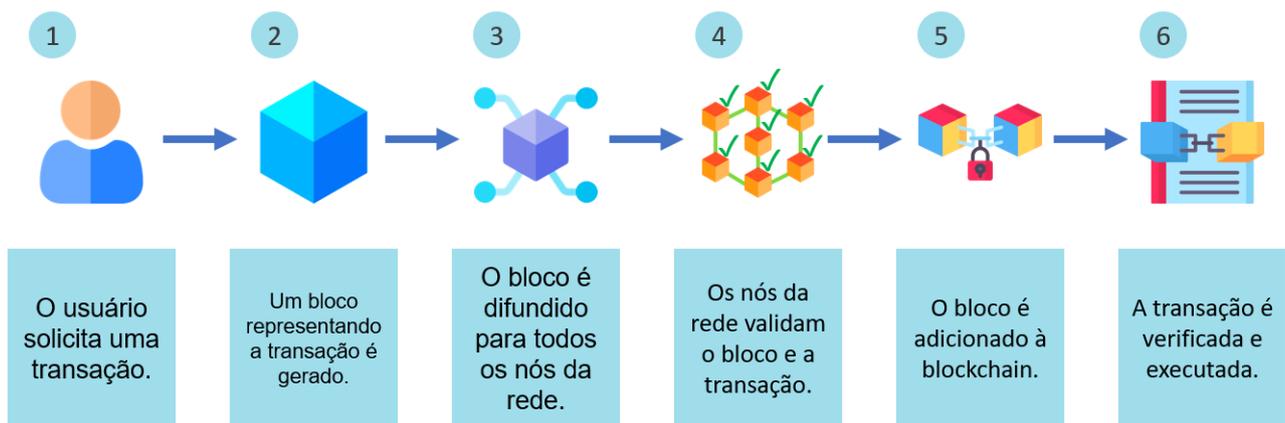
A Blockchain é uma tecnologia que vem sendo alvo de pesquisas e implementações nos mais diversos setores, inclusive no setor da saúde. Desde sua implementação para o desenvolvimento do Bitcoin a partir da publicação de seu *white paper* em 2008 Nakamoto, S., (2008), diversos estudos vêm sendo feitos para uma maior abrangência na sua utilização que vão além da área financeira. As vantagens potenciais da tecnologia Blockchain vão além do escopo econômico – se estendem a áreas políticas, humanitárias, sociais e também científicas – e a capacidade tecnológica proporcionada pela Blockchain está sendo explorada por grupos específicos das mais diversas áreas buscando a resolução de problemas do mundo real.

As pesquisas nessa área são relativamente novas e, diversos pesquisadores da área da informática estão investindo recursos para propor soluções eficazes. Nesse sentido, tal tecnologia permite o registro de dados de uma maneira confiável, com segurança, feita de forma distribuída e tolerante a falhas. Segundo Swan, M., (2015) a evolução da Blockchain pode ser compreendida em três fases, denominadas Blockchain 1.0, 2.0 e 3.0, cada

respectiva fase foi classificada a partir de inovações implementadas que possibilitaram uma evolução no que se refere a seu uso.

Sendo o Bitcoin a principal utilidade inicial da tecnologia, a possibilidade de trocas de moedas eletrônicas entre participantes da rede distribuída, sem que haja a necessidade de um terceiro ente centralizado e confiável. A Figura 1 ilustra o funcionamento de uma Blockchain, tal funcionamento é explicado na grande maioria das vezes utilizando os conceitos das criptomoedas, porém essa ideia pode ser ampliada para todas as áreas que a Blockchain pode atuar.

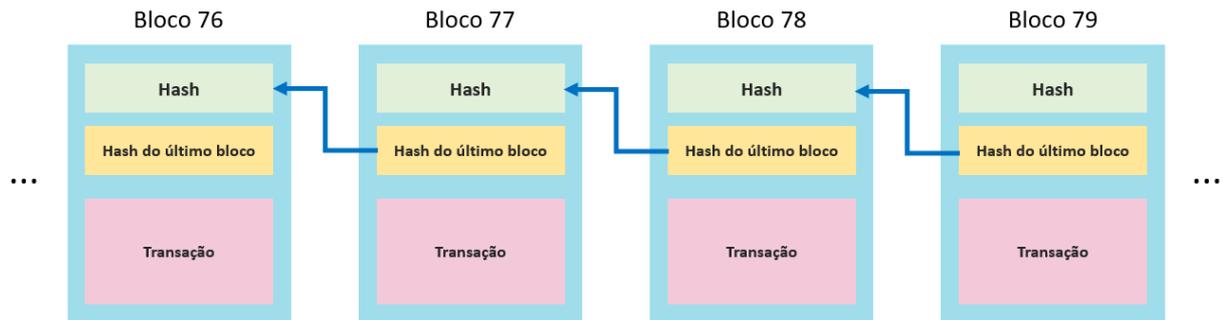
Figura 1. Funcionamento de uma Blockchain.



Fonte: Autor.

A rede Blockchain é formada por uma sequência de blocos, que possuem uma lista completa de registros de transações como um livro-razão-público convencional, de acordo com Lee Kuo Chuen, D. (2015). Como é ilustrado na Figura 2, cada bloco da rede aponta para o bloco anterior, utilizando para isso uma referência do bloco anterior, em um valor chamado *hash*, denominado bloco-pai. O primeiro bloco gerado em uma Blockchain é chamado bloco gênese, e não possui um bloco pai, os blocos seguintes apontam sempre para o bloco anterior a partir da referência do *hash*.

Figura 2. Blocos em uma rede Blockchain.

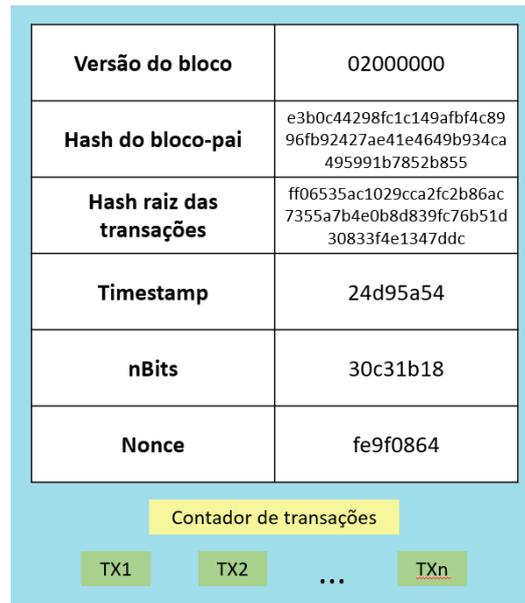


Fonte: Autor

Cada bloco é constituído por duas partes, um cabeçalho e o corpo do bloco. O cabeçalho possui a versão que define o conjunto de regras de validação do bloco seguinte. O valor do *hash* do bloco pai, composto por um valor de 256 bits que aponta para o bloco anterior. O valor-raiz da árvore *Merkle*, contendo o valor do *hash* de todas as transações do bloco. Um *timestamp* atual como segundos desde 1970-01-01T00:00 UTC. o *nBits*, um destino do *hash* atual compactado e o *Nonce*, composto por um campo contendo 4 bytes, começando por 0 e vai aumentando de acordo com cada *hash* calculado.

No corpo do bloco é o local onde ficam armazenadas as informações referentes às transações realizadas, podendo conter qualquer tipo de dados ou procedimentos. Na área financeira isso pode representar uma quantia ou movimentação de valores, em um setor como a saúde, isso pode representar algum formulário contendo dados médicos. Na Figura 3 é ilustrado cada componente citado.

Figura 3. Componentes do bloco.



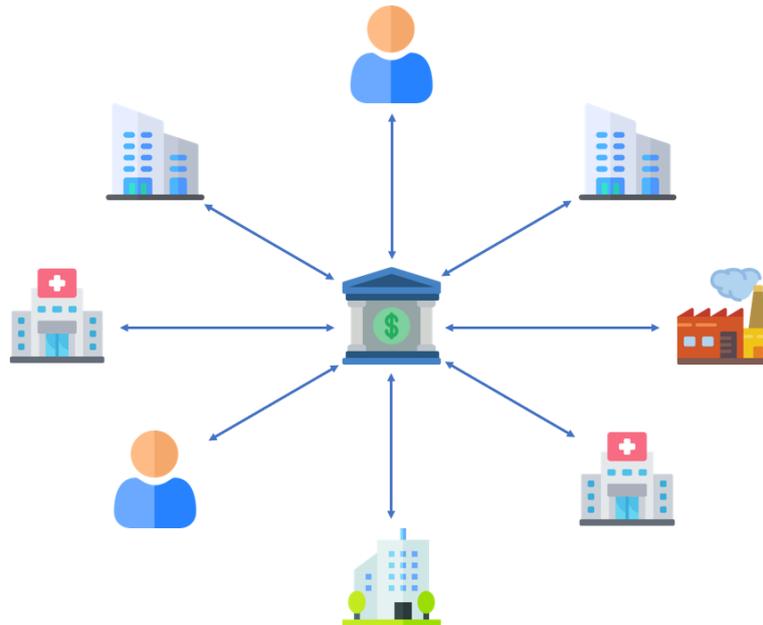
Fonte: Zheng, et al. (2018).

Após a criação de um novo bloco em uma rede Blockchain o mesmo é replicado para todos os dispositivos através de uma rede *peer-to-peer* (P2P) onde cada dispositivo pode atuar nessa rede como um cliente ou servidor e a comunicação ocorre de forma descentralizada.

Os objetivos iniciais da Blockchain eram dar suporte a transações de cunho financeiro, transações monetárias eletrônicas que envolvem pessoas e/ou empresas tradicionalmente possuem um terceiro participante confiável conhecido do inglês como *Trusted Third Party* (TTP), que faz a intermediação entre as partes, geralmente um banco faz o papel dessa terceira parte.

Um problema surge com a necessidade desse mediador, o mesmo precisa ser confiável, como esboçado na Figura 4. Todas as entidades necessitam de uma entidade central que possua um grau de confiança para realizar as transações entre elas, na Figura 4, a entidade confiável é representada por um banco.

Figura 4. Esquema centralizado de transações.



Fonte: Autor

Uma terceira parte não possui confiabilidade por diversos motivos, o mau funcionamento, falhas ou até mesmo um procedimento malicioso pode comprometer as transações, dessa forma o mediador compromete um sistema de transações a partir de um ponto de falha. Outras questões podem englobar a cobrança de taxas, tempo de espera, entre outros problemas.

O Bitcoin e a Blockchain surgem para superar esses problemas e propor um novo paradigma. Segundo Agbo, C. C. et al. (2019), um ano após a publicação do famoso *white paper* sobre o Bitcoin, a criptomoeda Bitcoin foi implementada, com o código liberado como código-fonte aberto, o que possibilitou que outros colaboradores que tivessem interesse, fizessem alterações no código, melhorando-o para criar diferentes gerações de blocos baseados em tecnologia Blockchain. Este avanço propiciou uma evolução na Blockchain que refletiu em três fases distintas que serão abordadas a seguir.

2.2. TECNOLOGIAS BLOCKCHAIN

A seguir serão apresentadas as gerações da tecnologia Blockchain e seus principais avanços.

2.2.1. BLOCKCHAIN 1.0

A primeira geração da Blockchain, chamada de 1.0 trata-se da invenção da tecnologia para dar suporte a criptomoeda Bitcoin, termo esse que muitas vezes é usado para se referir a três coisas que apesar de estarem relacionadas, são distintas, segundo Swan, M. (2015), primeiro, o termo Bitcoin se refere à plataforma de tecnologia Blockchain subjacente. Em segundo lugar, Bitcoin é usado para significar o protocolo que roda sobre a tecnologia Blockchain subjacente para descrever como os ativos são transferidos na Blockchain. Terceiro, Bitcoin também denota uma moeda digital, a primeira e maior das criptomoedas.

Essa primeira geração engloba desde o lançamento do *white paper* em 2008 por um indivíduo de pseudônimo *Satoshi Nakamoto*, que propunha uma solução para o problema de gasto duplo, que é um problema encontrado em moedas digitais, que até então, o dinheiro digital era como qualquer outro ativo digital que poderia ser infinitamente copiável Lamport, L. et al. (2014). A Blockchain resolve o problema de gasto duplo combinando a tecnologia de compartilhamento de arquivos ponto-a-ponto do BitTorrent com criptografia de chave pública para gerar uma nova forma de dinheiro digital. Essa primeira fase da Blockchain engloba toda essa etapa de implementação do Bitcoin e desenvolvimento do ecossistema que iria evoluir no mercado financeiro.

Desde sua concepção, a tecnologia Blockchain foi pensada para receber futuras implementações que viriam a evoluir sua capacidade e aplicabilidade, segundo o próprio Nakamoto em uma comunicação realizada em 2010, o design fornece suporte a uma vasta gama de formas de transações possíveis, que foram projetadas anos atrás, como contratos vinculados, arbitragem de terceiros, assinaturas multipartidárias, dentre outras formas de transações.

Com uma possível popularização do Bitcoin, essas serão possibilidades que podem ser exploradas no futuro, que tiveram que ser projetadas desde o início para permitir os futuros avanços Nakamoto, S. (2010). Dessa forma, as futuras pesquisas e implementações vieram a resultar no que seria classificado pela literatura como Blockchain 2.0.

2.2.2. BLOCKCHAIN 2.0

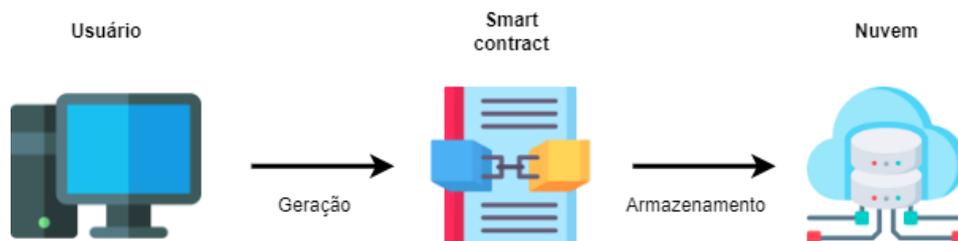
A Blockchain 2.0 é discutida pela literatura possuindo algumas diferenças em sua classificação, de acordo com Aggarwal, S. et al. (2021), o conceito de Blockchain 2.0 foi a

versão estendida do Blockchain 1.0 para um aplicativo mais interessante conhecido como *Smart Contracts*, que é definido como um protocolo automatizado computadorizado que é usado para facilitar, verificar ou aplicar digitalmente o acordo para a execução de um contrato legal.

Isso faz com que a necessidade de um elemento discutido anteriormente não seja necessária, a autoridade central, ou o terceiro participante, fazendo com que o contrato possua procedimentos que geram a validação de forma mais rápida econômica e segura dentro da plataforma da Blockchain, dispensando a autoridade central.

Em 1994, Nick Szabo um cientista da computação especialista em criptografia, onde é afirmado que os contratos inteligentes podem ser implementados com o auxílio do DLT denominado Blockchain Szabo, N. (1994). Nas Figuras 3 e 4 são ilustrados o funcionamento de um Smart Contract, esses contratos inteligentes podem ser implementados através de códigos armazenados e replicados em uma rede Blockchain que serão supervisionados pelos nós pertencentes a essa rede.

Figura 5. Funcionamento básico de um Smart Contract na nuvem.



Fonte: Autor

Na Figura 3 é esboçado o procedimento de execução de um smart contract na rede, definindo o fluxo da ordem de execução desde a criação do contrato, passando pela verificação de acordo com as regras pré-definidas para então ter seu registro na nuvem. Na Figura 4 é ilustrado com mais detalhes os procedimentos da geração do contrato inteligente, passando por cada respectivo estágio de sua execução.

Figura 6. Processos do Smart Contract.



Fonte: Autor

Em Aggarwal, S. et al. (2021) é feita uma comparação para o entendimento do funcionamento de um contrato inteligente. O paralelo é realizado com uma máquina de vendas automática, onde anteriormente teria a necessidade de um tabelião ou advogado para realizar o trâmite, e obter seus documentos, pagaria uma quantia enquanto iria aguardar o trâmite e a devolução dos documentos.

Com um Smart Contract o cliente simplesmente adiciona uma moeda na máquina de vendas (em paralelo ao terceiro participante), juntamente com a documentação, os próprios contratos inteligentes iriam definir as regras e procedimentos para que fossem validados. Essas e outras características fazem com que os contratos inteligentes sejam objetos de estudos e contínuos aperfeiçoamentos.

No entanto, existem algumas considerações acerca dos contratos digitais, que se diz respeito a legislação atual, segundo Efiging, A.C. et al. (2018) existem inúmeros desafios jurídicos impostos à realização dos smart contracts no Brasil, principalmente, porque inexistem leis específicas para tutela desta inovação contratual. Tendo em vista também a constante dinamicidade da tecnologia e a capacidade do Poder Legislativo brasileiro de acompanhar tais mudanças e evoluções da tecnologia, o que se pode tornar um desafio. No entanto, a tecnologia Blockchain vem se tornando cada vez mais popular, o que se faz

necessário o acompanhamento por parte das instituições públicas e privadas para que façam o melhor uso da tecnologia.

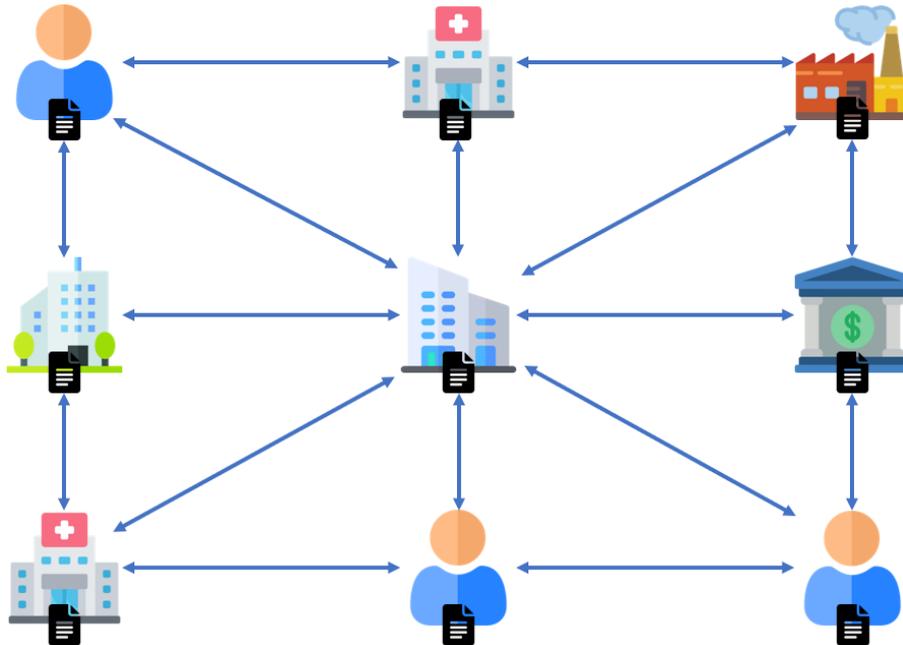
2.2.2.1. LIVRO RAZÃO DISTRIBUÍDO

Um conceito importante utilizado na Blockchain é o de Livro-Razão Distribuído do inglês, *Distributed Ledger Technology* (DLT), trata-se de uma base de dados descentralizada que é mantida pelos participantes da rede em que ela se encontra, onde não existe a necessidade de possuir confiança entre esses participantes (classificados como “nós”). Todos os nós possuem o mesmo grau de participação e direitos sobre a base de dados e possuem uma comunicação entre si através de uma arquitetura P2P para notificar atualizações no repositório. O mais comum é que tais atualizações sigam uma regra para que realizem apenas acréscimos no repositório, para garantir a imutabilidade dos dados contidos. Não existe a necessidade de uma autoridade central ou intermediadores nessa rede, sendo que os nós utilizam um algoritmo de consenso distribuído para acordar sobre as alterações que serão feitas no repositório.

Segundo Maesa, D.F. et al. (2020) existe uma divergência quanto ao termo livro-razão distribuído, sendo mais correto atribuir o termo *descentralizado*, uma vez que cada entidade da rede trabalha de forma independente, realizando tarefas distintas enquanto gera a comunicação dos resultados como dados para as outras entidades participantes. Para que fosse um livro-razão distribuído, cada nó deveria seguir um protocolo para realizar o mesmo resultado (toda vez que um consenso for atingido), sendo que cada participante honesto deve finalizar com a mesma cópia da base de dados. O que ocorre é uma replicação para cada participante sendo as mesmas operações de gerenciamento repetidas por todos a nível local.

Na Figura 7 é apresentado um esquema simplificado de um livro razão descentralizado, onde diversas entidades que podem ser de diversas origens possuem o mesmo direito sobre a rede Blockchain e possui ainda uma réplica do repositório, todas as entidades podem comunicar-se entre elas por P2P, onde cada nó dessa rede pode atuar tanto como cliente quanto como servidor, isso possibilita o compartilhamento direto de dados sem que haja a necessidade de um servidor ou repositório central.

Figura 7. Esquema de uma rede de livro-razão distribuída.



Fonte: Autor.

2.2.3. BLOCKCHAIN 3.0

Para entender o que viria a se tornar o Blockchain 3.0, é necessário entender que tal tecnologia poderia facilitar através de uma maneira computacional automatizada um número quase infinito de procedimentos e transações através de um sistema nunca antes imaginado na história humana. segundo Swan, M. (2015), todo e qualquer fenômeno que pode ser quantizado (definido em unidades ou pacotes discretos) pode ser denotado dessa forma, codificado e transacionado de forma automatizada na Blockchain.

Devido a essa possibilidade, segundo Maesa, D.F. et al. (2020), todas as aplicações da tecnologia Blockchain que se referem ao espectro mais amplo de usos de livros-razão distribuídos não relacionados a criptomoedas são comumente chamadas de aplicações Blockchain 3.0. A flexibilidade da tecnologia possibilita uma vasta gama de aplicações, proporcionando uma melhoria em diversas áreas, bem como criando uma abordagem completamente nova em outras áreas, que vão desde as criptomoedas como no início da tecnologia, atuando no setor econômico-financeiro, Internet das Coisas (*Internet of Things - IoT*), gestão de cadeias de suprimentos e o tema que será abordado com mais enfoque pelo seguinte trabalho, o uso da tecnologia no setor da saúde.

Os últimos anos foram marcados pela geração de um grande volume de dados, o termo Big Data surge nesse cenário, representando, de uma forma simplista, o grande volume de dados utilizados para a geração de informações, sejam elas estruturadas ou não. Indo além, como citado por Boyd, D. et al. (2011) as articulações em rede, assim como o aumento da velocidade e diversidade possibilitam a produção de mais dados a partir dos dados já existentes, seja sobre indivíduos, grupos ou ainda sobre a própria informação.

Da mesma forma que o Big Data possibilita a modelagem dos dados para garantir esquemas que auxiliam processos da realidade. O uso da tecnologia Blockchain pode auxiliar nas ações a serem tomadas. Como citado por Swan, M. (2015), a Blockchain pode ser unida ao Big Data a partir de camadas na transformação reativa para preditiva que está em andamento na ciência que estuda o Big Data com o intuito de automatizar operações em grandes áreas de tarefas através de contratos inteligentes e econômicos. O uso Smart Contracts juntamente com as análises preditivas proporcionadas por Big Data pode gerar uma grande economia de recursos, com a execução automática dos contratos.

Dessa forma, os diversos processos que podem ser quantificados e/ou armazenados, bem como transacionados e não estão nas gerações anteriores do Blockchain podem fazer parte do que é o Blockchain 3.0.

Acredita-se que a tecnologia dos Smart Contracts e a Blockchain podem ser utilizadas nos mais diversos campos que necessitem de contratos e trabalhos com ativos, bem como diversos tipos de transações. A seguir uma breve descrição de casos onde os contratos inteligentes podem ser utilizados para o beneficiamento.

- Gerenciamento: A tecnologia Blockchain oferece diversos recursos que podem ser utilizados para gerenciar e reduzir as diferenças que eventualmente ocorrem a partir de processamento independente e que podem custar tempo e recursos, além do mais fornece ainda o *Distributed Ledger Technology* (DLT) como uma fonte de confiança para que tais procedimentos sejam realizados.
- Governo: O combate à corrupção é uma preocupação recorrente dos governos e o uso de contratos inteligentes e da tecnologia Blockchain para garantir a segurança de procedimentos críticos ao governo, como uma eleição e/ou sistemas de votação que de forma tradicional dependem de uma autoridade central, sendo então que possui um ponto de falha. Com a utilização de Blockchain, os votos seriam protegidos no livro-razão distribuído, o que garantia um nível de segurança maior,

a decodificação dos dados necessita de um alto poder computacional, o que inviabilizaria ataques de hackers ou alterações no sistema de votação. Outra possibilidade proporcionada seria um sistema de votação online, o que iria reduzir custos.

- Imóveis: A tecnologia de livro-razão distribuído possibilita que corretoras e agência imobiliárias realizem pagamentos através de criptomoedas e implementem os contratos nos livros-razões públicos distribuídos o que reduz custos de intermediários nas transações.
- Saúde: A área da saúde pode se beneficiar muito com o uso de Blockchain e contratos inteligentes, a segurança proporcionada pela tecnologia pode garantir a confidencialidade de dados sensíveis, os Registros Eletrônicos de Saúde (RES) podem ser codificados e assegurados na rede Blockchain contendo uma chave privada, bem como os diversos procedimentos médicos que necessitam de confidencialidade, como resultados de exames, relatórios cirúrgicos, medicações, entre outros elementos. Podendo ainda gerenciar os Sistemas de Informações de Saúde (SIS) de forma mais sustentável e segura.

Como visto, diversas áreas podem se beneficiar com o uso dessa tecnologia, essa gama de aplicabilidades possibilitou sua evolução para o que viria a ser classificado como Blockchain 3.0.

Com a evolução tecnológica se desenvolvendo de forma a atender as necessidades das organizações, fatores como a globalização e o próprio mercado fizeram com que as organizações fizessem investimentos na implementação de sistemas ao longo dos tempos, para garantir eficiência e uma melhor gestão dos processos. Ainda assim, diversas empresas e instituições ainda mantêm um sistema legado por motivos particulares, tais sistemas normalmente não são totalmente compatíveis com sistemas externos, tornando-os muitas vezes defasados. Porém, evidências indicam diversos benefícios da integração dessas redes para uma saúde melhor e interconectada, necessitando a interconexão entre as várias organizações para pesquisadores na área da informática na saúde Lemieux, V.L. (2016).

3. ANÁLISE DO USO DA TECNOLOGIA BLOCKCHAIN NO SETOR DE SAÚDE

A seguir será apresentada uma análise, contendo na Subseção 3.1, os critérios utilizados na elaboração da pesquisa. Na Seção 3.2. será apresentada uma análise do estado da arte, contendo os trabalhos relevantes na revisão da literatura, que abordam de forma teórica o uso da Blockchain na saúde. Na Seção 3.3. será apresentada uma análise do estado da prática, contendo trabalhos relevantes que propuseram uma solução de software.

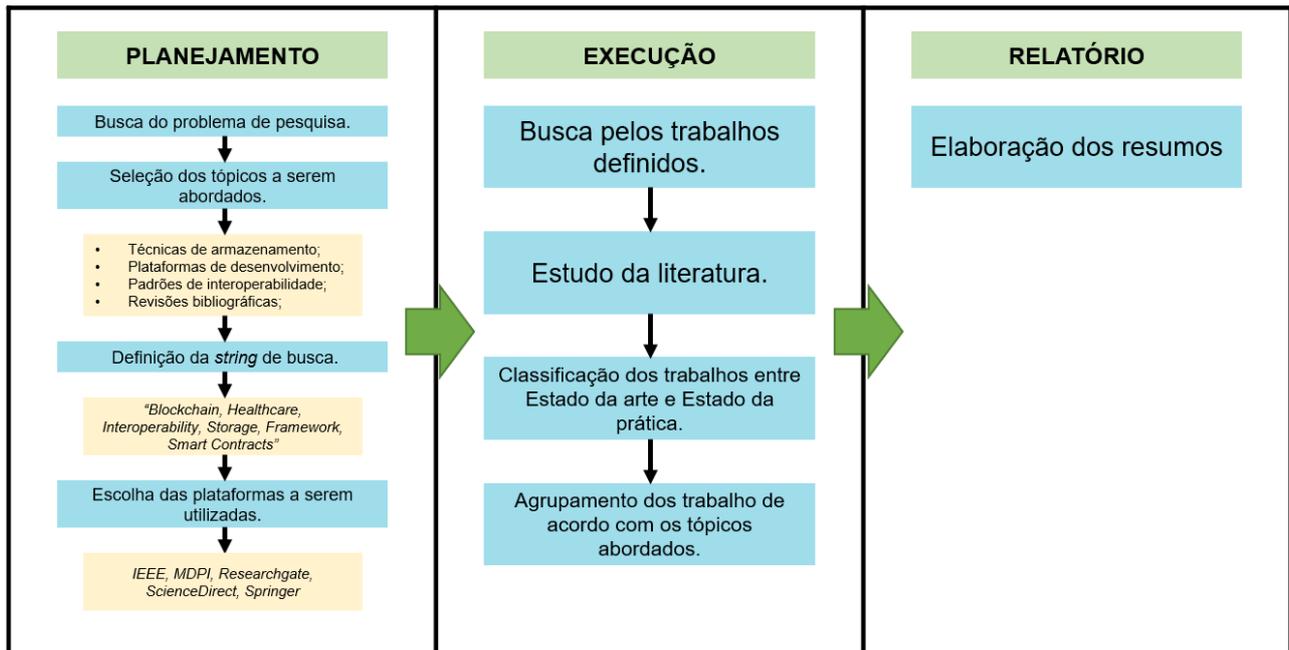
3.1. CRITÉRIOS ADOTADOS NA PESQUISA

Desde a implementação da tecnologia Blockchain, sua evolução vem possibilitando diversas pesquisas na área médica, uma evolução contínua que proporciona o avanço em diversos setores dentro da área. Nesse sentido, a partir da Subseção 3.2 serão descritos trabalhos do estado da arte e da prática que abordam o uso da Blockchain na área da saúde nos dias de hoje. Para a busca dos trabalhos foram utilizados alguns critérios, sendo eles:

- Disponibilidade dos artigos nas plataformas da IEEE, MDPI, Researchgate, ScienceDirect e Springer (Também foi utilizado artigo da Sociedade Brasileira de Computação como suporte);
- Data de publicação a partir de 2018 até a data presente;
- Abordagem do uso da Blockchain tendo em vista sua classificação podendo tratar sobre Técnicas de armazenamento; Plataformas de desenvolvimento e Padrões de interoperabilidade e contribuições no estado da arte, para isso foi definido uma *string* de busca contendo as seguintes palavras-chaves: *Blockchain, Healthcare, Interoperability, Storage, Framework*.

Os critérios utilizados são ilustrados na Figura 8, de acordo com a ordem utilizada na elaboração do planejamento de pesquisa.

Figura 8. Critérios de pesquisa esquematizado.



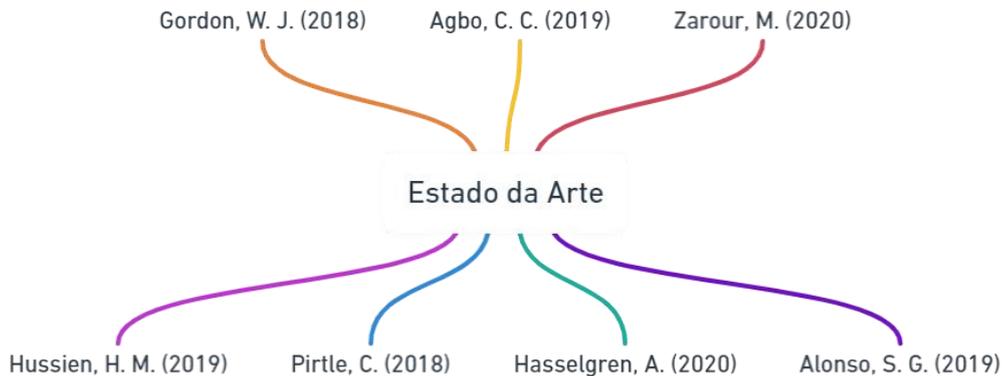
Fonte: Autor.

3.2. ANÁLISE DO ESTADO DA ARTE

Com base nos critérios citados na Subseção 3.1. foram analisados um total de trinta trabalhos, cada um sendo classificado com uma ou mais das áreas abordadas como ilustrado na Figura 8. Na Tabela 1, posteriormente, serão demonstrados os trabalhos analisados, juntamente com seu respectivo ano e sua temática de abordagem. A seguir serão discutidos os trabalhos identificados.

A importância da pesquisa no uso dessa tecnologia vem sendo cada vez mais evidente, os trabalhos que fazem uma revisão e análise do estado da arte demonstram como se encontra o estágio atual de desenvolvimento de soluções. Nesse sentido, foram considerados para o estado da arte, trabalhos que fazem uma revisão sistemática da tecnologia Blockchain e como ela está sendo aplicada no setor da saúde. Nesses trabalhos não são propostas soluções de software, na Figura 9 são ilustrados os trabalhos que seguem nessa abordagem.

Figura 9. Artigos do Estado da Arte.



Fonte: Autor.

No estudo de Hussien, H. M. et al. (2019) é realizada uma revisão sistemática no que se refere ao uso da tecnologia Blockchain na área da saúde, com o objetivo de fazer um mapeamento do cenário de pesquisa das tecnologias atuais. Para isso, os autores realizam a pesquisa em três bases de dados, sendo elas a *ScienceDirect*, *IEEE* e *Web of Science*, a partir dos resultados encontrados, os trabalhos são divididos em três categorias, sendo a primeira os trabalhos que propõem alguma aplicação que integra a Blockchain, nessa categoria são encontrados um total de 43 do total de 58 artigos. A segunda trata-se dos estudos relacionados à temática, que fazem a análise e avaliação da adoção da Blockchain nos sistemas de saúde, compreendendo um total de 6 artigos. A terceira e última categoria, trata-se dos artigos de revisão e pesquisas relacionados à temática, totalizando um total de 6 artigos.

Além da pesquisa, o trabalho oferece motivações e desafios que estão abertos a soluções sobre o uso da Blockchain, o que demonstra que apesar dos avanços nos estudos e desenvolvimento da tecnologia, ainda existem diversos campos e desafios a serem superados.

Tais desafios a serem resolvidos são também objetos de estudos, em Pirtle, C. (2018) os autores buscam demonstrar as dificuldades encontradas para a tecnologia Blockchain quando se trata de um sistema único contendo dados da área de saúde. Os autores definem a tecnologia e demonstram as dificuldades encontradas pela tecnologia Blockchain para a implementação de um sistema único contendo os RES, afirmando que devido ao desafio da manutenibilidade de uma rede de grande porte seria inviável para a

organização atual de sistemas de saúde, sendo a Blockchain uma ferramenta mais adequada para auxiliar outros processos que fazem parte da área da saúde.

Com base na evolução da tecnologia, diversas pesquisas buscam realizar uma análise geral de como se encontra o estado atual e criar pontos de partida para resolução de problemas recorrentes e possibilidade de novas áreas de estudo, buscando em bases contendo pesquisas com a temática.

A proposta dos autores em Hasselgren, A. et al. (2020) é também realizar uma revisão sistemática de publicações que utilizam ou propõem o uso de Blockchain para auxiliar em processos, serviços, pesquisas e educação na área da saúde. Os autores realizam uma revisão sistemática das publicações, tendo um total de 39 resultados, desses, as duas plataformas que mais possuem trabalhos nesse sentido são a *IEEE* com cinco papers publicados e *The Journal of Medical Systems* com seis papers publicados, dos trabalhos revisados, os anos das publicações partiram de 2016, contendo 4 publicações, 2017 contendo 11 publicações e 2018 contendo 23 publicações, sendo a maioria dos estudos originados de institutos de pesquisas da China, seguido por institutos americanos.

Os resultados demonstram que a maioria das pesquisas tratam de propostas de design estrutural, sendo 54% dos resultados, seguindo por novos algoritmos ou protocolos, representando assim 38% dos trabalhos. Os resultados do trabalho demonstram que existe um aumento significativo no campo das pesquisas que abordam o uso da Blockchain na área da saúde, tendo em vista propostas de resolução de diversos processos que englobam o setor.

Uma das possibilidades que estão sendo estudadas é a adoção do controle de segurança por parte do paciente, como demonstrado em Gordon, W. J. et al. (2018), cujo o objetivo é analisar como a tecnologia Blockchain pode facilitar a interoperabilidade orientada ao paciente através de cinco mecanismos: I) regras de acesso digital; II) agregação de dados; III) liquidez de dados; IV) identidade do paciente; e V) imutabilidade de dados.

Neste trabalho, os autores descrevem um problema encontrado na interoperabilidade dos dados de saúde. Em casos onde há mudança da interoperabilidade orientada à instituição para a interoperabilidade voltada ao paciente. E como o uso da tecnologia Blockchain pode resolver esse problema, nesse quesito, são apresentadas algumas barreiras encontradas. Como a barreira referente ao tamanho e volume de dados

clínicos, que vêm aumentando de forma exponencial, como mencionado por Fornel, D. et al (2018), por exemplo, uma única imagem de ressonância magnética cardíaca pode exigir 200 megabytes de armazenamento. O que torna inviável o armazenamento direto na cadeia de blocos devido a sua característica distribuída, outra questão é o tempo decorrido por causa da prova de trabalho realizada para a verificação de novas transações.

Outra barreira citada é a questão da privacidade e segurança, a identidade normalmente é ocultada pela chave pública na Blockchain, porém outros dados das transações são disponibilizados de forma pública, o que torna um problema. Existem implementações de Blockchain que buscam resolver esse problema, como a *Zcash*, uma criptomoeda que possui como principal característica o uso de criptografia para garantir a privacidade, ela permite a divulgação de forma seletiva de dados privados.

Existe também a questão do envolvimento do paciente, tal modelo de estrutura envolve mais o paciente do que um modelo orientado a uma instituição de saúde. Os pacientes precisam gerenciar seus dados, senhas, chaves e isso poderia necessitar de intermediários, o que não está definido ainda quem desempenharia essa função, sendo talvez uma oportunidade para o mercado, como ocorre com as criptomoedas. Outro desafio mencionado refere-se aos incentivos para uso da tecnologia.

Os autores propõem algumas soluções para os problemas discutidos anteriormente. Para o problema do volume de dados é proposto a troca das imagens e mídias completas por relatórios resumidos. O uso Blockchain em localizações geográficas locais, onde iriam lidar com os grandes volumes de dados sem a necessidade de validação intensiva de tempo.

Para o problema da segurança e privacidade é proposto o consórcio autorizado para membros para minimizar a exposição pública e o armazenamento de dados *off-chain*, com *on-chain* focado em permissões e outros metadados.

Para o problema de gestão de dados por parte do paciente, é proposto a criação de aplicações intermediárias para o paciente gerenciar chaves públicas e permissões. Por último, para o problema de incentivos é proposto a criação de incentivos federais para expandir a cobertura de API, também a associação de dados abertos com valor para reembolso e o fomento a competição de sistemas com APIs habilitadas para encorajar a sistemas a investirem em infraestrutura de API.

Outro trabalho a ser mencionado foi o artigo de Agbo, C. C. et al. (2019), onde autores realizam uma revisão sistemática da utilização da Blockchain na área da saúde, utilizando como base os Itens de Relatório Preferenciais para Revisões Sistemáticas e Meta-Análise, do inglês, *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) detalhando os estudos realizados, bem como o estado da arte no desenvolvimento de aplicações de Blockchain para saúde.

Neste trabalho, os autores utilizaram as diretrizes descritas na declaração PRISMA para elaboração da revisão sistemática, assim como o processo para estudo de mapeamento sistemático, com base no mapeamento foram identificados os casos de uso da Blockchain na área da saúde, da mesma forma que as aplicações desenvolvidas, e suas limitações, onde foram analisados 65 trabalhos.

Nos trabalhos identificados, os temas abordados foram o gerenciamento de registros médicos eletrônicos, gestão de cadeia de suprimentos farmacêuticos e de medicamentos, pesquisas e educação biomédica, monitoramento de pacientes de forma remota, análise de dados, entre outros tópicos.

Diversas soluções também foram desenvolvidas como protótipos utilizando paradigmas novos da Blockchain, como contratos inteligentes, Blockchain permissinado, armazenamento fora da cadeia, etc. Porém ainda é necessário investimento em pesquisas para complementar os esforços que vêm sendo feitos para resolver questões como escalabilidade, latência, interoperabilidade, segurança e privacidade. Essa pesquisa demonstra que métodos de estudo estão sendo utilizados de forma ampla para organizar o estado da arte.

Isso também pode ser demonstrado na publicação de Zarour, M. et al. (2020) é proposta uma avaliação de como a tecnologia Blockchain está impactando na área da saúde, principalmente quando refere-se a segurança dos RES, utilizando o método *Fuzzy Analytic Analytical Network Process* (F-ANP) para calcular os pesos dos critérios para sanar as divergências de opiniões de 56 especialistas que deram feedback sobre o tema, ainda foi utilizado a técnica *Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution* (TOPSIS) para avaliar o efeito de soluções alternativas.

A metodologia utilizada trouxe uma série de dados a serem analisados, os resultados obtidos auxiliaram os engenheiros a identificar e selecionar o modelo de Blockchain mais eficaz, contribuindo para um avanço no setor. Os métodos utilizados para realizar as

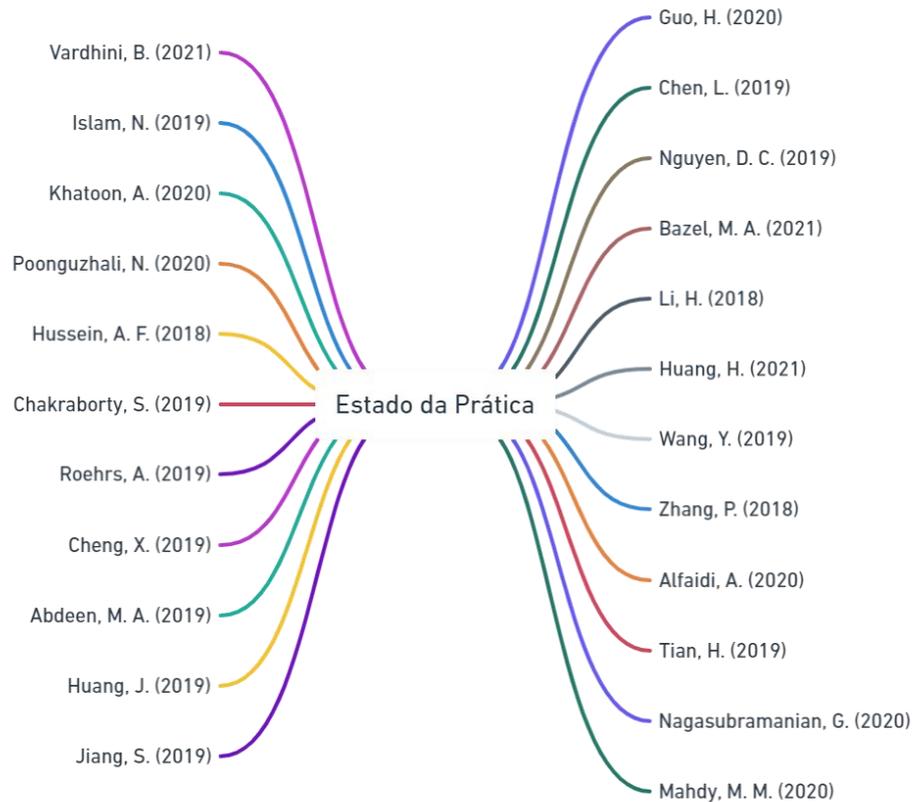
análises levaram em consideração características da Blockchain como descentralização, imutabilidade e segurança, dessa forma o modelo *Private Blockchain* se destacou como a opção de maior relevância, o que garantiu a primeira posição entre os modelos selecionados para fornecer segurança aos RES nas organizações de saúde. Uma rede Blockchain privada oferecia plataformas com mais segurança para o compartilhamento dos dados.

Com isso, pode-se perceber o crescente interesse da academia para com o uso da Blockchain na saúde, no trabalho de Alonso, S.G. et al. (2019) é realizada uma revisão do estágio atual de pesquisas que abordam o uso da tecnologia Blockchain aplicada em *e-health*. A busca dos estudos foi realizada utilizando bases públicas como *IEEE Xplore*, *Google Scholar*, *Science Direct*, *PubMed*, *Web of Science* e *ResearchGate*, impondo uma limitação de escopo do ano de 2010 até o ano presente do trabalho. Os resultados encontrados somaram um total de 84 publicações sobre Blockchain associada a *e-health*, dessas, 18 foram identificadas como possuindo uma grande relevância, 5,56% correspondem ao ano de 2016, 22,22% a 2017 e 72,22% a 2018, demonstrando um aumento significativo no interesse pelo tema.

3.3. ANÁLISE DO ESTADO DA PRÁTICA

Nessa seção serão discutidos os resultados referentes ao uso prático da tecnologia Blockchain em soluções de software na área da saúde. Tais soluções estão subdivididas em três abordagens, são elas: Técnicas de armazenamento; Padrões de interoperabilidade; e Plataformas de desenvolvimento. Sendo que a grande maioria das soluções propostas englobam mais de uma dessas categorias. Na Figura 10 são ilustrados os trabalhos analisados que fazem parte dessa classificação, os trabalhos serão discutidos à medida que os temas específicos serão abordados.

Figura 10. Trabalhos do Estado da Prática.



Fonte: Autor.

Abordando as plataformas de desenvolvimento, em Khatoon, A. (2020) o autor propõe o desenvolvimento de um sistema que utiliza contratos inteligentes para o gerenciamento de dados médicos que agilizam procedimentos médicos complexos.

Após realizar uma revisão sistemática com o intuito de entender as novas soluções na área da saúde, sendo algoritmos, métodos, metodologias ou arquiteturas o autor utiliza dados clínicos realistas para estudar a aplicabilidade da utilização da Blockchain nos diversos fluxos de trabalho de saúde, bem como a viabilidade de adoção atual da tecnologia em casos de uso distintos.

A proposta de solução trata-se de uma aplicação descentralizada (DApp) que utiliza uma rede Blockchain privada e um sistema de arquivos distribuídos no *back-end*. O sistema de contratos inteligentes foi implementado com uso do *Ethereum*, que utiliza o algoritmo de consenso denominado Prova de Trabalho, do inglês, *Proof of Work* (PoW) chamado *Ethash* que está sendo estudada a possibilidade de alteração para um algoritmo de Prova de

Participação, do inglês, *Proof of Stake* (PoS). Cada etapa do desenvolvimento foi registrada com uma linha do tempo para possibilitar auditoria.

Em um *Smart Contract*, seus principais elementos são eventos, funções, variáveis de estado e modificadores, os contratos foram escritos utilizando a linguagem de programação *Solidity*. A rede para realização dos testes foi *Remix*, *Kovan* foi utilizado para implantar os contratos *ethers testnet* e *testnet* para fazer o pagamento da taxa de transação. Os resultados atingidos demonstraram como os princípios de um sistema descentralizado podem ser utilizados de forma eficiente no ambiente médico para gerenciar grandes volumes de dados e tornar procedimentos complexos mais simples.

No trabalho de Poonguzhali, N. et al (2020) se propôs a criação de um RES utilizando Blockchain, onde são realizados dois processos, o primeiro é a criação do bloco e em seguida realizada um processo criptográfico utilizando o Algoritmo de Criptografia de Curva Elíptica (ECC), que utiliza recursos matemáticos de curvas elípticas para produção de sistemas com chave pública.

O sistema proposto foi implementado com o uso da plataforma Ethereum, os participantes do sistema foram definidos como sendo o paciente, o médico e um administrador, cada um com suas respectivas funções como adicionar, atualizar, excluir e visualizar.

Foram criados parâmetros de avaliação para o sistema, são eles o tempo de execução e a latência, para isso foi utilizado um banco de dados próprio. Com o aumento dos registros a escalabilidade proposta, juntamente com a imutabilidade foram mantidas, para segurança, foi assegurado que os dados do RES não fossem acessados por pessoas não autorizadas e para os dados que foram acessados por pessoas permitidas a privacidade ainda foi mantida, nas gerações dos blocos, o valor dos *hashs* atuais e anteriores foram calculados utilizando o algoritmo criptográfico ECC.

Existe um custo alto para a realização da Prova de Trabalho, diferentemente do tempo de verificação que é mais fácil, grande parte do processo do PoW é baseado no *hashing* onde cada bloco é aceito pelos membros da rede e o minerador realiza a prova de trabalho para que as transações ocorram. Com o passar do tempo, novas transações são geradas e adicionadas em seguida ao bloco já existente em um período de cerca de dez minutos, sendo um princípio fundamental do funcionamento da rede Blockchain.

No trabalho de Guo, H. et al. (2020), os autores propõem uma arquitetura de software híbrida com Blockchain e nós de bordas para facilitar o gerenciamento dos registros eletrônicos de saúde. A arquitetura proposta pelos autores utiliza a metodologia baseada em múltiplas assinaturas utilizando atributos (ABMS). Com o intuito de realizar autenticação de assinaturas dos usuários sem que seja necessário revelar informações confidenciais. Também foi implementado o esquema de criptografia baseado em atributos de múltiplas autoridades (ABE) com a finalidade de criptografar os dados dos RES que são armazenados no nó da borda.

O módulo Blockchain foi desenvolvido utilizando a plataforma *Hyperledger Fabric* e o módulo ABMS na biblioteca *Hyperledger Ursa*, os eventos de autenticação gerados e atividades de acesso foram registrados como transações no Blockchain do Hyperledger Fabric, o tempo de assinatura e verificação foi medido em diferentes configurações. Variando o comprimento dos atributos, o comprimento foi aumentado de 10 para 100, 1.000 e 10.000 caracteres e os resultados demonstraram que tanto o tempo de assinatura quanto de validação são independentes do comprimento do atributo, ficando em torno de 32ms a 243ms, respectivamente.

O artigo de Chen, L. et al. (2019) propõe a criação de um mecanismo de busca de dados que realize consultas através de um índice em um sistema com Blockchain, que garanta integridade e segurança dos dados, assim como a privacidade dos usuários, e também propor uma análise de performance a partir de dois aspectos, a saber, em termos da sobrecarga para extrair os *IDs* de documentos de RES e a sobrecarga associada à realização de transações em contratos inteligentes no Ethereum.

A metodologia utilizada na elaboração deste trabalho pode ser dividida em quatro etapas: A criação de um esquema de criptografia pesquisável baseado em Blockchain para o compartilhamento de RES, utilizando o potencial dos smart contracts como Ethereum. A utilização de expressões booleanas complexas para extrair os RES para construir os índices que diferencia dos esquemas usados na literatura, e ainda suporta consultas complexas que permitem que diferentes agentes de saúde solicitem permissão para acessar e interagir com os RES.

O contrato inteligente usado no esquema é projetado para rastrear recompensas monetárias, incluindo taxas de transação entre as partes envolvidas, garantindo que o proprietário dos dados seja pago desde que revele a transcrição, dessa forma, permitindo

que outros usuários pesquisem no banco de dados, garantindo justiça entre proprietários e usuários dos dados. Isso possibilita que os usuários dos dados possam receber os resultados da pesquisa de forma precisa, sem a necessidade de verificações adicionais. Como apenas o índice é migrado para o Blockchain, os RES reais precisam ser autenticados pelos proprietários dos dados, o que confere a ele o controle dos dados.

O processo de construção do índice compreende a extração de identificadores de documentos e o empacotamento desses identificadores para inclusão no contrato inteligente. Portanto, a sobrecarga de tempo da construção do índice consistiu em duas partes. No entanto, sem acesso a um banco de dados de RES disponível publicamente ou um hospital colaborador, não foi possível avaliar o desempenho real de abordagem proposta no trabalho. Na prática, a sobrecarga de tempo é principalmente incorrida no contrato inteligente, e, portanto, é eficiente para o proprietário dos dados. Aproveitando o Blockchain, o esquema proposto atinge a justiça no sentido de que os usuários honestos (e não a entidade maliciosa) serão recompensados. A análise de segurança e as avaliações de desempenho sugeriram que o esquema proposto é viável e eficaz.

Os autores em Li, H. et al. (2018) propõem a implementação de um sistema de preservação de dados *Data Preservation System* (DPS) baseado em Blockchain, com a finalidade de oferecer uma solução de armazenamento confiável que garanta a verificabilidade e primitividade dos dados armazenados, preservando a privacidade dos usuários.

Os autores propõem um novo sistema de preservação de dados médicos baseado em Blockchain, para fornecer uma solução de armazenamento confiável que garante que os dados armazenados não sofrerão adulterações, que faz ainda a verificação da validade dos dados e garante a privacidade aos usuários. Utilizando o conceito de prova de primitividade dos dados, o que significa que as características dos dados serão armazenadas e preservadas para sempre no Blockchain utilizando a plataforma Ethereum. Os resultados provindos da avaliação do desempenho demonstram que o custo para a preservação utilizando o DPS proposto é inferior a US \$2, independentemente se o tamanho dos arquivos armazenados seja de 50 MB. Sua vantagem em comparação com os sistemas eletrônicos gerais para preservação de dados é que ele pode lidar com situações onde os dados são facilmente perdidos e/ou adulterados, garantindo que mesmo

em casos onde o banco de dados seja adulterado ou danificado, os dados ainda podem ser recuperados por meio da rede Blockchain.

O trabalho de Zhang, P. et al. (2018) se propõe a realizar quatro contribuições para o estado da arte no uso da tecnologia Blockchain na área da saúde, a primeira é uma análise dos requisitos do Roteiro de Interoperabilidade Compartilhada Nacional do Escritório do Coordenador Nacional de Tecnologia da Informação em Saúde (ONC) e suas implicações para sistemas que utilizam Blockchain. Segundo a apresentação do FHIRChain, trata-se de uma arquitetura baseada em Blockchain que atende os requisitos do ONC, encapsulando o padrão *HL7 Fast Healthcare Interoperability Resources* (FHIR) e, terceiro, é a proposta de uma solução descentralizada baseada no FHIRChain e por último um análise de estudo de caso.

Os autores utilizaram como base para o trabalho, os requisitos técnicos definidos no “*Shared Nationwide Interoperability Roadmap*”, DeSalvo, K.B. (2015) elaborado pelo Escritório do Coordenador Nacional de Tecnologia da Informação em Saúde (ONC), ainda foi apresentada uma arquitetura baseada em Blockchain denominada FHIRChain, que atende aos requisitos propostos pelo ONC. O FHIRChain utiliza elementos da dados FHIR do HL7 (que possuem tags de identificação exclusiva) em conjunto com um design baseado em token para trocar recursos de dados de forma descentralizada e verificável, sem exigir esforços duplicados de upload de dados para um repositório centralizado.

Como proposta de aplicação, foi desenvolvida uma solução descentralizada baseada no FHIRChain, que faz o uso de identidades digitais para realizar a autenticação dos pacientes e gerar autorizações de acesso aos dados. A aplicação desenvolvida possibilita o compartilhamento de informações específicas e estruturadas, aumentando a flexibilidade nas opções de compartilhamento.

No estudo de caso, foi constatado que a solução pode ser estendida para oferecer suporte a outros requisitos técnicos, melhorando problemas de interoperabilidade e também foram explorados os problemas de troca de dados que a Blockchain ainda possui limitações e utilizando como problemas de pesquisas futuras.

A proposta de Abdeen, M. A. et al. (2019) trata-se de uma arquitetura globalmente integrada de compartilhamento de RES, baseada em Blockchain e *HL7 client*. Sendo que os RES são armazenados nos países hospedeiros e não na Blockchain. Essa arquitetura disponibiliza registros médicos de pacientes em viagem temporariamente e após realizar a

autenticação necessária. O processo de autorização real é executado em um sistema de gerenciamento de identidade federado, como o *Shibboleth*. Embora haja semelhanças, o sistema proposto difere, pois, envolve o paciente no processo de permissão e revela a ele a identidade das entidades acessadas em seus registros de saúde. Dessa maneira, apresentar uma arquitetura que utiliza o conceito de gerenciamento de identidade federado, disponibilizado pela FIDM. Usando ainda a tecnologia Blockchain para garantir segurança e imutabilidade.

Inicialmente, vários problemas são apontados, como por exemplo, o problema de comunicação entre os diversos sistemas em caso de um armazenamento globalmente distribuído, ou a incapacidade de rastrear dados quando o paciente necessitar ir a um hospital ou clínica que não tenha cadastro prévio. A solução para esse problema é permitir alterações nos registros de assistência médica apenas mediante consenso entre todas as partes envolvidas. Os autores apresentam uma arquitetura que utiliza o conceito de gerenciamento de identidade federado, disponibilizado pelo *Federated Identity Management* (FIDM) juntamente com a segurança proporcionada pelo Blockchain.

O HL7 fornece uma federação de sistemas de saúde em todo o mundo. Ou seja, se um paciente estiver viajando entre países e necessitar de serviço de saúde, ele poderá acessar seus registros de saúde de qualquer lugar. O provedor de serviços remotos será capaz de recuperar o RES do paciente de seu banco de dados local, ao mesmo tempo em que evita a violação desses registros. O modelo apresentado é baseado em três módulos, o cliente HL7, a estrutura *Shibboleth* para fornecer gerenciamento de identidade e o Blockchain para fornecer transações confiáveis e imutáveis.

Foi usado o *Hyperledger Composer* para desenvolver o cliente HL7 com a rede Blockchain autorizada. O cliente HL7 solicita ao servidor HL7 que posteriormente autorize com um IdP. Havendo clientes *NodeJS* disponíveis que solicitam e analisam os dados do servidor HL7. Na implementação da prova de conceito, foi conectado o módulo *composer-client* npm para criar um arquivo de rede de negócios (BNA). Quando o cliente recebe os dados, ele distribui os dados do cliente em várias tabelas do *CouchDB*.

No entanto, cada transação é encadeada com a rede Blockchain. Cada transação de saúde é registrada e qualquer alteração nos registros pode ser facilmente detectada no banco de dados. O cliente obtém as informações da estação doméstica usando a identidade do usuário, como a identidade do passaporte. Em seguida, ele gera um URL de solicitação

e se comunica com o servidor HL7 para enviar/receber/analisar mensagens HL7. Os registros de saúde do paciente acessados pelo serviço remoto são temporários e são excluídos após o descarte do paciente. No entanto, o livro razão do Blockchain mantém um *hash* criptografado desse registro para verificação de integridade e processo de consenso. Em Huang, J. et al. (2019) é apresentada uma solução denominada *MedBloc*, um sistema de RES baseado em Blockchain que permite que pacientes e provedores de saúde acessem e compartilhem registros de saúde, preservando a privacidade. No *MedBloc*, os RES são armazenados em uma rede Blockchain e criptografados de maneira que ninguém, além do paciente e os provedores de saúde confiáveis autorizados possam visualizá-los ou atualizá-los. Utiliza um sistema de gerenciamento de consentimento para o prestador de serviço de saúde em que os pacientes podem controlar quais prestadores podem acessar os RES, para isso utiliza-se contratos inteligentes que reforçam as regras de controle de acesso. Os recursos criptográficos utilizados para proteger ou fazer o compartilhamento dos registros é gerenciado através de um serviço de autenticação para evitar que os usuários percam ou exponham os recursos a pessoas não autorizadas.

O objetivo do trabalho de Nagasubramanian, G. et al. (2020) é a criação de um framework que utiliza sua infraestrutura em nuvem de assinatura sem chave (KSI) junto ao armazenamento descentralizado com a Blockchain, gerando o sistema denominado *Blockchain KSI* (KSIBC). A metodologia utilizada foi uma análise do estado da arte e da prática, buscando identificar trabalhos que abordam os seguintes temas: Atributo e técnica de criptografia baseada em identidade, Técnica de criptografia hierárquica, Arquiteturas de saúde, Arquitetura existente baseada em Blockchain, Protótipo *MedRec*, Infraestrutura de assinatura sem chave (KSI) e Blockchain.

Também foi proposta a implementação de uma infraestrutura, buscando a privacidade e a integridade dos dados, o sistema proposto neste artigo executará o compartilhamento dos registros apenas se houver valores correspondentes parcialmente baseados em atributos. Isso é feito usando acesso anônimo, compartilhando apenas as informações comuns e, em seguida, diferenciando as informações altamente seguras usando valores de atributo.

Uma tecnologia abordada é a Blockchain KSI que nada mais é que a junção das duas tecnologias (a Blockchain e o KSI). KSI é uma infraestrutura de assinaturas sem chaves baseado na função *hash*. A tecnologia Blockchain KSI fornece privacidade,

segurança e integridade de dados. Os dados são assinados e armazenados no Blockchain KSI. Posteriormente, em algum momento, os dados são verificados para sua assinatura com a hora assinada. Como não há chaves no KSI como no sistema de criptografia pública, o KSI não pode ser comprometido. KSIBC é uma técnica descentralizada e distribuída que facilita a adição de novos registros.

Ao usar a assinatura digital e a técnica de Blockchain, a integridade dos dados é garantida em grande parte no framework KSIBC proposto. A aplicação adicional da Blockchain garante que os dados possam ser parcialmente adicionados como blocos para que um carimbo de data / hora possa ser gerado para os dados sendo armazenados ou atualizados, o que também aborda o recebimento do bloco específico. Para usar esse recurso de Blockchain, os usuários da nuvem precisam pagar uma pequena taxa aos provedores e mineradores pela prestação de serviços.

No trabalho de Wang, Y. et al. (2019) o intuito é propor um protocolo de compartilhamento de RES seguro, que garanta a privacidade do usuário, baseado em Blockchain, utilizando criptografia pesquisável e criptografia de proxy condicional para realizar a segurança dos dados e o controle de acesso.

Os autores propõem uma nova estrutura para o armazenamento de RES, através da computação em nuvem, que possibilita o compartilhamento e garante a privacidade e segurança dos dados, utilizando o consórcio da Blockchain. A nuvem garante o armazenamento do texto cifrado dos RES dos pacientes, enquanto a Blockchain mantém os registros do texto cifrado da palavra-chave de pesquisa e compartilhamento dos dados. Além disso, foi projetada uma prova de autorização como mecanismo de consenso para a rede Blockchain. No esquema proposto, apenas os solicitantes autorizados que possuem um alçapão de pesquisa têm permissão para buscar as palavras-chave e as informações relacionadas, propondo ainda a implementação no *Hyperledger Fabric* e melhorias nos contratos inteligentes como trabalhos futuros.

A proposta de trabalho de Tian, H. (2019) é a criação de uma chave compartilhada que possibilite a reconstrução pelas partes legítimas antes do processo de diagnóstico e tratamento, criptografando e armazenando os dados em uma Blockchain usando a chave compartilhada. Essa solução atende os requisitos de integridade, disponibilidade e privacidade dos dados médicos.

Para resolver dois problemas típicos dos RES convencionais, que são eles, a integridade dos dados que são armazenados em bancos de dados locais, que mesmo possuindo um controle de acesso ainda podem ser modificados ou excluídos, e outro problema é a criptografia de dados médicos onde a chave é atribuída ao paciente, sendo que essa chave não pode ser compartilhada, quando o paciente morre os dados ficarão indisponíveis. A proposta de uma chave compartilhada utilizando as famílias de funções intratáveis irmãs (SIFF) vem para estabelecer uma chave compartilhada e o uso do *Hyperledger Fabric* para armazenar dados criptografados. Através dos testes foi validada a eficiência da proposta.

Referindo-se aos padrões de interoperabilidade, tal conceito representa a capacidade de criar uma comunicação eficiente entre os diferentes sistemas. Muitas vezes estão relacionados a uma padronização no armazenamento de dados, para que sigam um modelo que seja interpretável por sistemas distintos, de forma eficaz.

Em Vardhini, B. et al. (2021) é proposta a criação de uma infraestrutura de grande porte que possibilite o acesso aos contratos inteligentes gerados patrocinados pelos RES como sendo os mediadores de informações. Devido a rede Blockchain possuir uma natureza descentralizada, isso tornará os RES acessíveis em uma rede de grande escala, isso ajudará na evolução dos Sistemas de Informação na área de saúde, fornecendo segurança, privacidade e rapidez nos pagamentos.

Os autores visam solucionar o problema da falta de consistência que existe devido às organizações de saúde possuírem os prontuários médicos de forma fragmentada, para isso, a solução proposta é hospedar as transações dos RES na Blockchain, criando um ecossistema inteligente. Somando a isso, fornecer o acesso aos dados do paciente de forma segura, evitando que terceiros não desejáveis acessem sem a devida autorização. As partes interessadas em obter acesso terão que solicitar permissão para ter acesso ao histórico do paciente e com isso gerar a transação no livro-razão distribuído.

Diversos recursos foram implementados, como uma delimitação de tempo para o acesso aos RES. A capacidade do paciente interagir com diferentes partes interessadas no acesso aos dados e mesmo assim manter sua privacidade, para isso, foi utilizado o mecanismo de prova de conhecimento zero. Uma técnica de criptografia onde determinado usuário prova possuir o conhecimento de uma informação sem revelar de forma explícita a informação conhecida.

Os próprios autores sugerem como melhoramentos futuros a permissão que os prontuários possam ser acessados em situações de emergência de forma rápida, e uma modificação na estrutura para adequação a uma enfermidade específica ou sendo modelada em padrões estabelecidos.

No trabalho de Islam, N. et al. (2019) é oferecida uma estrutura para monitorar e fazer o reconhecimento de atividades humanas, que possa ser utilizado em hospitais, para isso utiliza o procedimento de categorização cooperativa multiclasse para aperfeiçoar a precisão da classificação das atividades nos vídeos que suportam o uso da Blockchain baseada em névoa, ou computação em nuvem.

A classificação das atividades capturadas em vídeos é realizada utilizando o algoritmo de aprendizagem de máquina denominado Máquina de Vetores de Suporte, do inglês, *Support Vector Machine* (SVM), baseado na estrutura de códigos de saída de correção de erros (ECOC). O objetivo central do seguinte trabalho é realizar o reconhecimento das atividades humanas em qualquer ambiente, esse reconhecimento é realizado em tempo real e através de vídeo que suportem a arquitetura de nuvem ou névoa baseada em Blockchain. Nos resultados foi observado que a abordagem proposta consegue ser mais eficiente e alcança maior precisão no reconhecimento das atividades humanas se compararmos com outras abordagens que realizam o reconhecimento de ações.

Em Hussein, A. F. et al. (2018) os autores propõem a implementação de um sistema suportado por uma *Transformada Wavelet Discreta* com o intuito de aumentar a segurança geral, juntamente com uma técnica de Algoritmo Genético para melhorar a técnica de otimização de filas. O projeto permite uma maior responsabilidade uma vez que todos os usuários do sistema são conhecidos e a rede Blockchain registra o *log* das transações.

Para a realização do trabalho, é adotada uma *Transformada Wavelet Discreta* para a sessão criptográfica com o objetivo de gerar uma chave descriptografada de *hash* único, em uma *Transformada Wavelet* (WT) para obter uma resolução criptográfica de baixa frequência e de melhor qualidade, são empregadas janelas de tempo longo, no entanto, para obter informações de alta frequência, são empregadas janelas de tempo curto. A utilização da *Transformada Wavelet* propicia um novo formato de chave a partir de *Strings MD5*, o que aumenta a segurança geral do sistema contra diversos tipos de ataques, durante a fase de descriptografia o tempo de processamento pode aumentar.

Ao realizar uma comparação entre os resultados obtidos com a solução proposta contra as soluções baseadas em Blockchain, o sistema proposto apresenta uma maior escalabilidade, robustez e imunidade a ataques, permitindo o compartilhamento seguro dos dados. Através da solução proposta é possível realizar o compartilhamento de dados sensíveis por vários ambientes de trabalho como clínicas, hospitais e centros de saúde, tendo ainda como propostas futuras a capacidade de controle em ambiente de nuvem o que possibilita uma expansão do sistema.

Em Chakraborty, S. et al. (2019) é realizada uma fusão de áreas relativamente novas da tecnologia da informação, a Internet das Coisas, *Machine Learning* e a rede Blockchain para o desenvolvimento de um sistema seguro. Com o objetivo de utilizar os dispositivos de IoT para interceptar e capturar dados dos pacientes, o Blockchain é usado para armazenar e manter esses dados na forma de múltiplas transações, tendo ainda um controle de acesso para as partes interessadas. O *Machine Learning* é usado para detectar anomalias e prever alguns cenários que possam surgir com base nos parâmetros repassados pelos médicos. O módulo de IoT monitora o paciente durante algum procedimento, esse monitoramento irá gerar um grande volume de dados, o armazenamento desses dados precisa ocorrer de forma segura.

Para isso, foram definidas duas redes Blockchain, uma para os cuidados de saúde pessoais e outra para o gerenciamento de registros externos, respectivamente *Personal Health Care (PHC) Blockchain* e *External Record Management (ERM)*. Os dados ainda podem ser acompanhados pelo médico para acompanhamento do paciente, esses dados gerados pelos dispositivos são armazenados em um banco de dados na nuvem e regulados por uma rede Blockchain. O sistema se mostrou eficaz no que se refere ao acompanhamento dos dados gerados, bem como na garantia de segurança proporcionada pela tecnologia.

Em Nguyen, D.C. et al. (2019) os autores propõem uma estrutura de compartilhamento de RES que utiliza Blockchain e o protocolo Sistema de Arquivos Interplanetário (IPFS) em uma plataforma de nuvem móvel. O seguinte trabalho visa propor uma arquitetura nova que possibilita o compartilhamento de RES utilizando Blockchain e o protocolo IPFS para um sistema de *e-health* em uma plataforma móvel, com o objetivo de melhorar a segurança no compartilhamento dos RES ainda foi desenvolvido um sistema de

controle de acesso utilizando contratos inteligentes. O protocolo de compartilhamento foi projetado para gerenciar o acesso do usuário ao sistema de RES.

O desempenho do modelo proposto foi investigado através de testes de usabilidade em uma aplicação *Android* na nuvem fornecida pela *Amazon Web Services (AWS)*, o que demonstrou a viabilidade para diversos cenários de *e-health*. Por fim, uma análise de segurança foi realizada, demonstrando as diversas vantagens do sistema proposto, os resultados obtidos mostram que a estrutura proposta pode permitir que usuários médicos compartilhem dados médicos em ambientes de nuvem móvel de maneira confiável e rápida, em comparação aos esquemas convencionais.

A proposta do trabalho de Bazel, M. A. et al. (2021) é explorar a capacidade de uso da Blockchain para a melhoria na gestão de *Big Data* na área da saúde, fornecendo uma visão do uso da tecnologia, bem como os desafios enfrentados. Algumas das características da Blockchain auxiliam no trabalho com *Big Data*, o tempo de processamento pode ser reduzido devido a disponibilidade oferecida no livro-razão distribuído que logo quando o paciente se inscreve no sistema, todos os dados ficam disponíveis de uma vez. Os médicos e/ou as partes interessadas podem acessar os dados originais, de forma precisa em tempo real, não precisando ter a preocupação da procedência dos dados, o que pode minimizar riscos de erros médicos.

Os autores listam os benefícios notáveis para o uso da Blockchain no gerenciamento de big data, dentre os benefícios estão a segurança e privacidade, a interoperabilidade e a capacidade de compartilhamento global de dados, a precisão de dados, a redução no custo de processamento de dados e a possibilidade de recorrer a uma auditoria de forma otimizada.

O objetivo do artigo de Huang, H. et al. (2021) é propor a criação de um sistema de *e-health* baseado em Blockchain, o sistema é denominado BCES, seu propósito é garantir que a manipulação dos RES possa ser auditada. No BCES, cada manipulação de consulta legítima de consumidores de dados, junto com cada manipulação de terceirização legítima de hospitais, será gravada na Blockchain como uma transação para armazenamento permanente, o que garante a rastreabilidade.

O BCES é um sistema de saúde eletrônico assistido por nuvem, usando Blockchain para registrar informações operacionais desde a geração de dados até o armazenamento em nuvem. O trabalho aqui apresentado, não conseguiu chegar a 100% do seu objetivo

final. O atual sistema médico eletrônico assistido por nuvem combinado com o Blockchain tem alguns problemas não resolvidos, como a incapacidade dos usuários de controlar seus próprios dados médicos, riscos ocultos de segurança no compartilhamento de dados de RES e proteção irracional da integridade dos registros.

A análise de segurança demonstrou que o BCES pode se defender contra diferentes tipos de ataques por meio de controle de acesso refinado e recursos de resistência à violação. Enquanto isso, a avaliação de desempenho foi conduzida para provar que o esquema é eficiente e viável. Como trabalho futuro, espera-se o melhoramento da estrutura de design por meio do uso de IA e tecnologia de aprendizado profundo, que será usada para combinar diferentes RES do mesmo tipo para melhorar a precisão do diagnóstico e tratamento de doenças sem revelar informações de dados reais.

O trabalho de Cheng, X. et al. (2020) propõe um modelo de rede *Medical Cyber Physical Systems* (MCPS) baseado em Blockchain, para garantir que os dados armazenados não possam ser violados e não rastreáveis.

Um MCPS consiste de um *Cyber Physical Systems* (CPS), um sistema inteligente onde os procedimentos são monitorados e controlados por algoritmos. Nesse esquema, a primeira etapa é garantir a segurança no armazenamento dos dados médicos, para isso utilizando a tecnologia Blockchain e fazendo o compartilhamento dos dados de forma segura, sendo necessária a criação de um esquema de rede.

O seguinte trabalho busca resolver a ameaça de segurança durante o processo de comunicação e autenticação, utilizando mapeamento bilinear e problemas intratáveis, em seguida, a lógica BAN é usada para analisar os protocolos de segurança, essa lógica auxilia a determinar se as informações trafegadas são confiáveis. Também foi realizada uma análise de forma e comparação dos protocolos de segurança.

Os resultados obtidos demonstram que o MCPS utilizando Blockchain realiza não apenas o compartilhamento de dados, mas também consegue suprir vários requisitos de segurança na fase de autenticação, tendo ainda custos indiretos de armazenamento aceitáveis, o que demonstra uma eficácia do esquema para o compartilhamento de *Big Data*.

A proposta do trabalho de Alfaidi, A. et al. (2020) consiste em uma investigação, projeção e implementação de sistemas de saúde móveis e seguros, tendo em vista o desenvolvimento de um sistema de *Health Record Chain* (HRC), que aproveita o uso de

mecanismo de autenticação e geolocalização utilizado pelos dispositivos móveis. Propondo ainda a resolução do problema de conflito entre o uso da Blockchain e sua característica da imutabilidade e o “direito de ser esquecido” garantido pela Regulamentação Geral de Proteção de Dados (GDPR).

Na solução proposta, um contrato inteligente é gerado para cada usuário que for cadastrado no sistema, esse contrato terá as informações do usuário, como o endereço *Ether*, ao momento que o contrato de autorização for implementado, fará com que os dados do RES do usuário sejam salvos com segurança em um banco de dados externo. O endereço *Ether*, junto com os dados do usuário serão salvos no banco de dados externo, o método de criptografia ABE foi utilizado para criptografar os dados do usuário no banco de dados, sendo que nesse caso, o usuário pode editar e deletar seus dados quando precisar.

Os resultados demonstraram que o HRC implementado melhorou a qualidade e a quantidade de dados para pesquisas médicas, o que torna um incentivo para os desenvolvedores utilizarem Blockchain nos sistemas. O HRC evita que os dados que estejam fora da cadeia encontrem o problema de escalabilidade da Blockchain. Ao tempo mesmo, para salvar o direito de privacidade do usuário, dando ainda o direito de remover todos os registros médicos.

Dessa forma o paciente controla seus dados dos RES, sabendo onde serão salvos e quem terá acesso a eles. Trazendo ainda a proposta da integração de uma Blockchain a ser utilizada na gestão de dados e solicitações do usuário, propondo uma investigação do uso de funções *hash* que possibilitem a edição e exclusão dentro da Blockchain como trabalhos futuros.

No artigo de Jiang, S. et al. (2019) é proposta a criação de uma Blockchain de consórcio (PESchain), onde os RES dos pacientes são criptografados e armazenados nas instituições médicas através de uma rede local, os valores dos *hashs* dos registros são armazenados no PESchain, sendo ainda implementado um esquema de autorização furtivo para a autorização de acesso na rede Blockchain, com o intuito de permitir o compartilhamento dos registros.

A solução proposta permite o compartilhamento dos RES de forma controlada pelo paciente, utilizando Blockchain para garantir tal procedimento. O esquema de autorização de forma anônima foi implementado para obter a entrega da autorização de acesso preservando a segurança durante o compartilhamento dos dados, ainda foi considerado

realizar operação de exclusão dos RES na rede Blockchain, no processo de empacotamento dos dados, os valores do *hash* dos RES são empacotados de acordo com diferentes tipos, e o bloco é excluído. O PESchain desenvolvido trata-se de uma rede simulada de forma local. Foi utilizado o *Ganache* para avaliar o desempenho, que se demonstrou positivo, a análise de segurança demonstrou que o PESchain consegue atender aos requisitos de segurança dejesados.

Em Mahdy, M. M. (2020) é proposto uma arquitetura de um sistema que utiliza um modelo de armazenamento de sistemas descentralizados em um sistema centralizado para possibilitar alta disponibilidade de dados dos sistemas distribuídos.

Permitindo ainda um nível elevado de segurança com implementação de autorização e autenticação dos sistemas centralizados. A Blockchain é usada para garantir a segurança e o pseudoanonimato dos pacientes, mantendo um registro dos RES compartilhados entre as entidades de saúde.

A solução sugerida é um sistema semi-centralizado composto entre sistemas distribuídos centralizados e sistemas P2P descentralizado, o intuito dessa arquitetura é diminuir os problemas atuais no referente aos RES tradicionais, essa arquitetura pode ser utilizada para implementação de sistemas que permitem o compartilhamento seguro dos dados, tendo ainda a possibilidade de receber melhorias na área de design de sistemas de registros eletrônicos de saúde.

Tais soluções se propõem a resolver diversos desafios da implementação de sistemas de informação que utilizam Blockchain. Como mencionado por (Zhang, P., 2018), soluções eficazes que utilizam essa tecnologia ainda precisam superar alguns desafios.

4. RESULTADOS E DISCUSSÕES

A seguinte sessão possui como objetivo realizar uma discussão a partir dos resultados obtidos na pesquisa, apresentando uma visão abrangente sobre tais resultados. Realizando ainda uma investigação dos temas de interesse sobre o uso da tecnologia Blockchain no setor da saúde.

Como foi demonstrado, o uso da tecnologia Blockchain é relativamente recente, desde sua primeira aparição em 2008, sua ascensão trouxe novas abordagens a áreas da Tecnologia da Informação. Sendo um tema muito discutido em diversos setores no mercado, na indústria e na academia.

As pesquisas realizadas visam contribuir com a evolução dessa tecnologia, trazendo melhorias e/ou novas soluções. O setor da saúde é um dos que mais vem se beneficiado com as pesquisas, diversos procedimentos que fazem parte do setor são abordados nessas pesquisas.

Na **Tabela 1** serão demonstrados os respectivos trabalhos e classificados de acordo com sua abordagem nas temáticas propostas, cada trabalho será referenciado a partir da citação do autor principal, juntamente com o ano de publicação. As siglas referem-se respectivamente a:

- A: Técnicas de armazenamento
- D: Plataformas de desenvolvimento
- I: Padrões de interoperabilidade
- R: Revisão da literatura

Tabela 1. Classificação dos trabalhos.

Nº	ARTIGO	A	D	I	R
1	Vardhini, B. (2021)	✓		✓	
2	Islam, N. (2019)	✓		✓	
3	Khatoun, A. (2020)	✓	✓	✓	
4	Poonguzhali, N. (2020)	✓	✓		
5	Hussein, A. F. (2018)	✓		✓	
6	Chakraborty, S. (2019)	✓		✓	
7	Hussien, H. M. (2019)				✓
8	Roehrs, A. (2019)	✓	✓	✓	
9	Guo, H. (2020)	✓	✓	✓	

10	Chen, L. (2019)	✓	✓	✓	
11	Pirtle, C. (2018)				✓
12	Nguyen, D. C. (2019)	✓		✓	
13	Hasselgren, A. (2020)				✓
14	Gordon, W. J. (2018)				✓
15	Agbo, C. C. (2019)				✓
16	Bazel, M. A. (2021)	✓		✓	
17	Li, H. (2018)	✓	✓		
18	Huang, H. (2021)	✓		✓	
19	Wang, Y. (2019)	✓	✓	✓	
20	Cheng, X. (2019)			✓	
21	Zarour, M. (2020)				✓
22	Zhang, P. (2018)		✓	✓	
23	Abdeen, M. A. (2019)	✓	✓	✓	
24	Alfaidi, A. (2020)	✓			
25	Huang, J. (2019)	✓	✓	✓	
26	Tian, H. (2019)	✓	✓	✓	
27	Jiang, S. (2019)			✓	
28	Alonso, S. G. (2019)				✓
29	Nagasubramanian, G. (2020)	✓	✓	✓	
30	Mahdy, M. M. (2020)	✓			

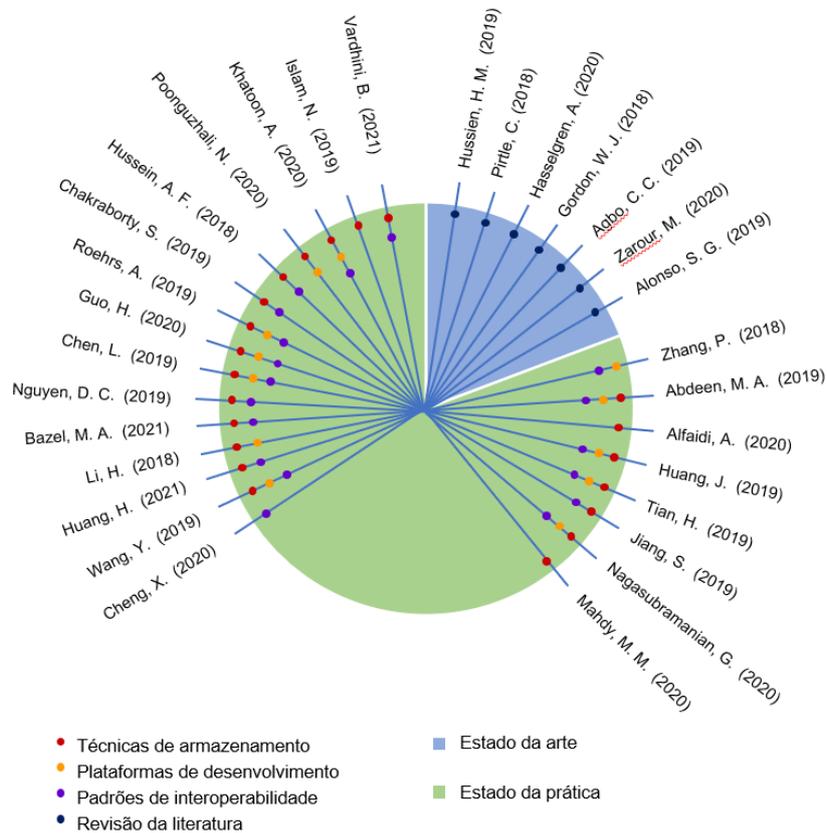
O primeiro ano utilizado como parâmetro para busca foi 2018, onde foram encontrados um total de sete trabalhos publicados. Para o ano seguinte, de 2019 foram localizados um total de treze trabalhos publicados. Em 2020 houve um total de nove trabalhos publicados e em 2021 um total de três publicações, levando em consideração que foram utilizadas cinco plataformas para busca dos trabalhos, sendo elas *IEEE*, *MDPI*, *Researchgate*, *ScienceDirect* e *Springer*.

É possível notar que as temáticas que ocorrem mais abordagens são técnicas de armazenamentos e padrões de interoperabilidade, onde diversas publicações abordam ambas as temáticas em conjunto somando um total de dezesseis publicações. Isso

demonstra o interesse da comunidade de pesquisa em busca de soluções que resolvam os problemas atuais de armazenamento, incluindo áreas como computação em nuvem Nguyen, D. C. et al. (2019) e análise de Big Data Bazel, M. A. et al. (2021).

Também são buscadas soluções que garantam uma comunicação eficiente entre os diferentes sistemas de informações, seja usando padronizações internacionais de dados (Roehrs, A., 2019) ou utilizando esquemas de buscas alternativos (Nagasubramanian, G., 2020). No Gráfico 1 é possível analisar quais trabalhos estão classificados em suas propostas.

Gráfico 2. Classificações dos trabalhos.



Fonte: Autor.

Na área azul estão os trabalhos ligados ao estado da arte. Tais trabalhos propõem revisões teóricas sobre a temática e identificando soluções que vêm sendo estudadas e implementadas. Totalizam sete trabalhos que possuem essa perspectiva, esses trabalhos também mostram as possíveis áreas que as pesquisas podem se direcionar. Demonstrem

que nos últimos anos houve um aumento significativo nas pesquisas envolvendo Blockchain. Na área verde estão os trabalhos ligados ao estado da prática, que propõem soluções que envolvem as classificações anteriormente citadas, totalizando vinte e três trabalhos nessa categoria.

Dessas publicações vinte e um abordam técnicas de armazenamento, propondo soluções para problemas como tempo de respostas e disponibilidade dos dados, bem como controle de acesso por parte dos usuários. Doze trabalhos abordam plataformas de desenvolvimento, sendo a plataforma descentralizada *Ethereum* a mais utilizada para execução dos contratos inteligentes. Por último, dezoito trabalhos discutem sobre padrões de interoperabilidade, sendo que a maioria das publicações tratam mais de uma dessas temáticas.

As publicações que tratam sobre o estado da arte descrevem diversas características da tecnologia Blockchain que podem auxiliar no setor da saúde, desde sua capacidade de segurança da rede devido a sua característica de descentralização até a garantia de privacidade dos usuários. Pode-se notar também que os artigos que analisam o estado da arte buscam identificar quais direcionamentos estão sendo tomados nas pesquisas, como em (Hussien, H. M., 2019) onde é feita uma análise de como estão as pesquisas para apontar desafios ainda existentes.

Nos trabalhos do estado da prática foram propostas diversas aplicações que utilizam outros campos da tecnologia da informação como o uso de dispositivos móveis, computação em nuvem, internet das coisas e análise de *Big Data*.

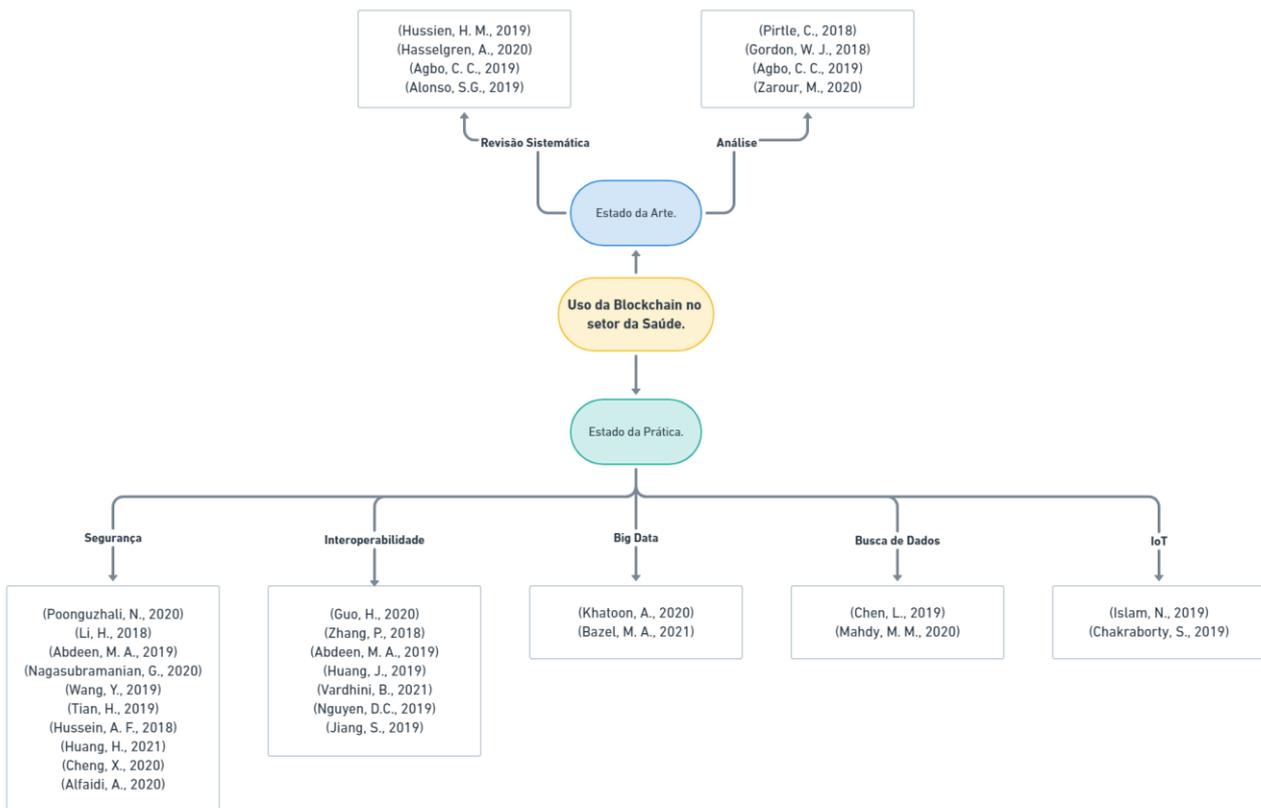
Essa fusão com outras áreas da tecnologia da informação demonstra a ampla aplicabilidade do uso da Blockchain, para os vários processos que englobam a área da saúde, desde o monitoramento de pacientes, como feito por (Chakraborty, S., 2019), sendo uma proposta que disponibilizaria um grande volume de dados a serem processados, o gerenciamento de grandes volumes de dados, como em (Bazel, M. A., 2021) também se beneficiaria com o uso da Blockchain.

Um dos fatores mais recorrentes trata-se dos RES e propostas de interoperabilidade entre sistemas, um desafio que diversos pesquisadores abordam, buscando soluções de realizar uma padronização dos dados a serem armazenados e uma forma de compartilhar tais dados de forma segura com as organizações de saúde e as partes interessadas que possuem autorização para tal. O controle permissionado por parte do paciente está sendo

discutido como uma solução a ser adotada por várias propostas, sendo essa uma característica dessa tecnologia que chama atenção dos pesquisadores, sendo uma tendência nas pesquisas atuais.

A Figura 11 ilustra um fluxograma contendo as respectivas áreas de foco de cada trabalho analisado.

Figura 11. Classificação dos temas principais de cada trabalho.



Fonte: Autor

É possível observar que nos trabalhos do estado da prática, revisões sistemáticas são as principais propostas, com o intuito de entender o cenário atual e para onde estão sendo direcionados os esforços de pesquisas, seguido por análises que buscam identificar características que a tecnologia Blockchain pode auxiliar no setor.

No estado da prática, é possível notar que a questão da segurança é o tópico que possui mais interesse nas pesquisas analisadas, isso se dá ao fato do crescimento do interesse e da utilização da tecnologia no setor, o que traz como consequência, pessoas

que procurar burlar o sistema. Em segundo lugar a interoperabilidade dos sistemas, que ocorre pelo número de sistemas de informação que são implementados e a falta de padronização entre esses sistemas. Ambos são problemas do setor que precisam de uma atenção devido ao seu grau de necessidade, pelo crescimento do setor.

Em seguida, temas como *Big Data*, busca de dados e IoT possuem o mesmo número de trabalhos de interesse, isso demonstra o quão a Tecnologia da Informação vêm se aperfeiçoando e buscando resolver problemas recorrentes e futuros como a capacidade de obter dados de dispositivos remotos e como tratar a grande quantidade de dados gerados da melhor forma.

4.1. OPORTUNIDADES E DESAFIOS NO ESTADO DA ARTE

Com base nos resultados da análise, é possível ter uma visão de como a tecnologia Blockchain vem sendo abordada no estado da arte, tanto para propor uma nova visão a ser trilhada, quanto para analisar os problemas e desafios que ainda precisam ser trabalhados e superados.

Alguns desafios ainda precisam ser superados quando se discute o uso de sistemas que utilizam Blockchain, desafios que vem sendo estudados e implementados de maneira rápida, muito se dá ao fato da liberdade de implementação propiciada pela Blockchain.

- **Capacidade de evoluir:** Um sistema de informação deve ser pensado de forma que consiga evoluir, tanto em questões de arquitetura e projeto, que possa receber novos recursos, quanto para questões de adequação a novas medidas e leis que eventualmente possam surgir, um sistema que possibilite tal evolução com o mínimo de alterações possíveis é uma solução ideal a ser buscada.
- **Armazenamento:** Um dos pontos cruciais para um bom funcionamento de uma rede Blockchain é a capacidade de armazenamento utilizada. Isso permite que a Blockchain seja armazenada nos dispositivos que estão ligados à rede, pois irão armazenar um grande volume de dados ligados aos pacientes, aos profissionais de saúde e as instituições envolvidas, dentre outros elementos que eventualmente possam fazer parte do sistema, dessa forma, a infraestrutura deve ser considerada no planejamento da rede.
- **Privacidade:** A privacidade é uma questão chave a ser tratada quando se refere aos sistemas de saúde, diversas condições devem ser levadas em consideração, como

questões de autenticação e permissionamento das partes interessadas, formas de criptografia e armazenamento eficiente dos dados, controles de acesso e visualização das informações, entre outras questões que estão sendo buscadas para eliminar as vulnerabilidades da tecnologia.

Em uma rede Blockchain, os dados estão dispersos entre os dispositivos participantes da rede, isso é um risco a ser considerado, pois para garantir que tais dados sejam seguros existe um processo de criptografia dos dados, caso esse processo seja burlado, o sistema poderá ser comprometido. Outro ponto a ser discutido trata-se dos contratos inteligentes que estão sendo executados na rede, que necessitam de atenção, pois suas funções podem ser auditadas e caso algum participante descubra algum erro de segurança, pode comprometer os demais participantes da rede.

- **Escalabilidade:** A escalabilidade consiste no número de transações que o sistema pode realizar em um determinado período de tempo, quando referimos ao setor da saúde, essas transações podem ser de diversos tipos, desde registros eletrônicos de saúde até armazenamento de imagens e exames clínicos. No desenvolvimento de um sistema com Blockchain, a escalabilidade é um ponto a ser considerado na sua implementação, o que pode resultar em decisões como a escolha de uma plataforma de desenvolvimento mais adequada como Ethereum ou Hyperledger.

Tais desafios apresentados podem ser utilizados como motivação para futuras pesquisas, análises que avaliem os pontos críticos da tecnologia Blockchain de forma específica, trazendo a literatura de como tais problemas possam ser sanados.

O interesse pela área vem se tornando crescente, somado a isso, o fato da tecnologia ser relativamente recente ainda abre muitas possibilidades de campos para análise e revisão da Blockchain.

4.2. OPORTUNIDADES E DESAFIOS NO ESTADO DA PRÁTICA

Quando referimos ao estado da prática é possível perceber que algumas das áreas que foram discutidas no estado da arte estão sendo trabalhadas com soluções que procuram resolver os desafios apresentados e ainda propõem novos paradigmas e casos de uso para a tecnologia.

A fusão de áreas do conhecimento vem proporcionando tais soluções, o uso de mecanismos de segurança sofisticados, incluindo criptografia, geração de chaves, autenticação e permissionamento de usuários, visam garantir uma maior eficiência nos sistemas. Propostas que utilizam dispositivos de Internet das Coisas expandem a maneira de obter dados e possibilitam uma gama de novos casos de uso, somado a isso, trabalhos que usam Blockchain para garantir a privacidade e segurança desses dados sensíveis são contribuições significativas para o desenvolvimento do setor.

Outra questão a ser tratada é uma forma de processar de maneira eficiente a grande quantidade de dados gerada nos mais diversos procedimentos que englobam o setor da saúde, essa quantidade de dados tende a aumentar cada vez mais, o que demanda soluções eficazes para tratar esse problema. Nesse sentido, a tecnologia Blockchain também vem sendo utilizada para sanar tais desafios, soluções que garantam a disponibilidade dos dados de forma rápida e com o custo reduzido são grandes oportunidades.

Outro ponto importante que foi demonstrado como um dos tópicos mais abordados, trata-se da interoperabilidade, a capacidade de comunicação e transferência entre os diversos sistemas existentes. Essa característica pode ser classificada de duas formas, a interoperabilidade funcional que foca na comunicação entre os sistemas utilizando regras de negócios e a interoperabilidade semântica, que visa compreender o significado dos dados envolvidos nas transações.

Para resolver essa questão, diversas propostas utilizam padronizações internacionais de dados, que estão ligadas aos RES. O objetivo dessas padronizações é uniformizar os dados dos registros, eliminando divergências entre diferentes sistemas, padrões como openEHR, HL7 e FHIR são usados para realizar essa uniformização das informações.

A segurança é um objetivo primordial que motiva o uso da tecnologia Blockchain no setor da saúde, isso foi demonstrado através das análises realizadas, e foi o tópico de foco mais proposto nos trabalhos analisados. Tendo em vista que cada vez mais soluções estão sendo implementadas, a tendência que o uso da Blockchain seja cada vez mais comum nos sistemas de informação de saúde, dessa forma, o foco na segurança e privacidade dos dados é um dos principais motivos que possibilitará a evolução dos sistemas.

5. CONCLUSÃO

A seguinte sessão possui os aspectos conclusivos do trabalho, sendo organizada da seguinte maneira. Seção 5.1 Considerações Finais, contendo uma visão geral acerca dos resultados discutidos na pesquisa. Seção 5.2 Indicações de Trabalhos Futuros.

5.1. CONSIDERAÇÕES FINAIS

O seguinte trabalho realizou uma análise dos aspectos mais relevantes considerados em pesquisas com o uso da tecnologia Blockchain no setor da saúde. Para isso foi feita uma pesquisa no estado da arte e da prática, trazendo trabalhos que abordam a temática de forma teórica e prática.

O seguinte trabalho busca trazer como principais contribuições um mapeamento das pesquisas que estão sendo feitas com a Blockchain na saúde, demonstrando os tópicos de interesse dos pesquisadores e como tais soluções podem contribuir para o desenvolvimento do setor, somando ao estado da arte e propondo caminhos para a realização de novas pesquisas.

Com base no que foi apresentado, o objetivo do trabalho foi alcançado de tal forma que os resultados encontrados foram utilizados se demonstraram eficazes para realização do mapeamento das pesquisas e elaboração das propostas de trabalho.

5.2. TRABALHOS FUTUROS

Como propostas de trabalhos futuros, é possível evoluir o estado da arte trazendo pesquisas que busquem propor soluções teóricas e práticas que venham a resolver desafios ainda existentes em áreas como segurança, armazenamento, privacidade e comunicação eficiente entre sistemas.

REFERÊNCIAS

1. Spínola, M., & Pessôa, M., **“Tecnologia da informação. In Gestão de operações: a engenharia de produção a serviço da modernização da empresa”**. São Paulo: Edgard Blücher/Fundação Vanzolini, 1997.
2. da Conceição, A. F., Rocha, V. M., & de Paula, R. F., **“Blockchain e Aplicações em Saúde”**. Sociedade Brasileira de Computação, 2019.
3. Pinochet, L.H.C., **“Tendências de Tecnologia de Informação na Gestão da Saúde”**. O Mundo da Saúde, São Paulo, 2011.
4. Nakamoto, S., **“Bitcoin: A Peer-to-Peer Electronic Cash System”**. 2008. Disponível online: www.bitcoin.org (Acesso em 26 de dezembro de 2021).
5. Swan, M. (2015). **“Blockchain: Blueprint for a new economy”**. " O'Reilly Media, Inc."
6. Lee Kuo Chuen, D. **“Handbook of digital currency”**. Elsevier, 2015.
7. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. **“Blockchain challenges and opportunities: A survey”**. International Journal of Web and Grid Services, 14(4), 352-375, 2018.
8. Agbo, C. C., Mahmoud, Q. H., Eklund, J. M., **“Blockchain Technology in Healthcare: A Systematic Review”**, Department of Electrical, Computer and Software Engineering, University of Ontario Institute of Technology, Canada, 2019.
9. Lamport, L., R. Shostack, and M. Pease. (1982). **“The Byzantine Generals Problem.”** ACM Transactions on Programming Languages and Systems 4, no. 3: 382–401; Philipp (handle). (2014). **“Bitcoin and the Byzantine Generals Problem—A Crusade Is Needed? A Revolution?”** Financial Cryptography. <http://financialcryptography.com/mt/archives/001522.html>; Vaurum (handle name). (2014). **“A Mathematical Model for Bitcoin.”** (blog post). <http://blog.vaurum.com/amathematical-model-for-bitcoin/>.
10. Nakamoto, S., **“Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG.”**, Bitcointalk, 2010. Disponível online: <https://bitcointalk.org/index.php?topic=195.msg1611#msg1611>. (Acesso em 27 de dezembro de 2021).
11. Aggarwal, S., Kumar, N., **“Blockchain 2.0: Smart contracts”**, Thapar Institute of Engineering and Technology, vol: 121, pp: 301-322 , India, 2021.

12. Szabo, N., **"Smart Contracts"**, 1994. Disponível online: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>. (Acesso em 27 de dezembro de 2021).
- 13.
14. Efig, A.C., Santos, A.P., **"Análise dos Smart Contracts à Luz do Princípio da Função Social dos Contratos no Direito Brasileiro"**, Direito & Desenvolvimento, Vol. 9, Nº 2, João Pessoa, 2018.
15. Maesa, D.F., Mori, P., **"Blockchain 3.0 applications survey"**, Journal of Parallel and Distributed Computing, 138, 99–114, Pisa, 2020.
16. Boyd, D. Crawford, K., **"Six Provocations for Big Data"**, Symposium on the Dynamics of the Internet and Society, Oxford, 2011.
17. Lemieux, V.L., **"Trusting records: Is Blockchain technology the answer?"**, Rec. Manag. Journal, Vol. 26, 110–139, 2016.
18. Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B., **"A systematic review for enabling of develop a Blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction"**. Journal of medical systems, 43(10), 1-35, 2019.
19. Pirtle, C., & Ehrenfeld, J., **"Blockchain for healthcare: The next generation of medical records?"**. Journal of Medical Systems, 42(9), 1-3, 2018.
20. Hasselgren, A., Kravlevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A., **"Blockchain in healthcare and health sciences—A scoping review"**. International Journal of Medical Informatics, 134, 104040, 2020.
21. Gordon, W. J., & Catalini, C., **"Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability"**. Computational and structural biotechnology journal, 16, 224-230, 2018.
22. Fornell D, Zagoudis J., **"Cardiac MRI advances. Diagn Interv Cardiol"**, 2016. Disponível online: [https:// www.dicardiology.com/article/cardiac-mri-advances](https://www.dicardiology.com/article/cardiac-mri-advances), Acesso em 27 de dezembro de 2021.
23. Zarour, M., Ansari, M. T. J., Alenezi, M., Sarkar, A. K., Faizan, M., Agrawal, A., ... & Khan, R. A., **"Evaluating the impact of Blockchain models for secure and trustworthy electronic healthcare records"**. IEEE Access, 8, 157959-157973, 2020.

24. Alonso, S. G., Arambarri, J., López-Coronado, M., & de la Torre Díez, I., "**Proposing new Blockchain challenges in ehealth**". *Journal of medical systems*, 43(3), 1-7, 2019.
25. Khatoon, A., "**A Blockchain-based smart contract system for healthcare management**". *Electronics*, 9(1), 94, 2020.
26. Poonguzhali, N., Gayathri, S., Deebika, A., & Suriapriya, R., "**A framework for electronic health record using Blockchain technology**". In 2020 International Conference on System, Computation, Automation and Networking (ICSCAN) (pp. 1-5). IEEE, 2020.
27. Guo, H., Li, W., Meamari, E., Shen, C. C., & Nejad, M., "**Attribute-based multi-signature and encryption for ehr management: A Blockchain-based solution**". In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-5). IEEE, 2020.
28. Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N., "**Blockchain based searchable encryption for electronic health record sharing**". *Future generation computer systems*, 95, 420-429, 2019.
29. Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S., "**Blockchain-based data preservation system for medical data**". *Journal of medical systems*, 42(8), 1-13, 2018.
30. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T., "**FHIRChain: applying Blockchain to securely and scalably share clinical data**". *Computational and structural biotechnology journal*, 16, 267-278, 2018.
31. DeSalvo, K. B., Re: "**Connecting health and care for the nation: A shared nationwide interoperability roadmap**". *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, 2015.
32. Abdeen, M. A., Ali, T., Khan, Y., & Yagoub, M. C. E., "**Fusing identity management, HL7 and Blockchain into a global healthcare record sharing architecture**". *Int J Adv Comput Sci Appl*, 10, 630-636, 2019.
33. Huang, J., Qi, Y. W., Asghar, M. R., Meads, A., & Tu, Y. C., "**MedBloc: a Blockchain-based secure EHR system for sharing and accessing medical data**". In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 594-601). IEEE, 2019.
34. Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., & Balusamy, B., "**Securing e-health records using keyless signature infrastructure**".

- Blockchain technology in the cloud**". Neural Computing and Applications, 32(3), 639-647, 2020.
35. Wang, Y., Zhang, A., Zhang, P., & Wang, H., "**Cloud-assisted EHR sharing with security and privacy preservation via consortium Blockchain**". IEEE Access, 7, 136704-136719, 2019.
36. Tian, H., He, J., & Ding, Y., "**Medical data management on Blockchain with privacy**". Journal of medical systems, 43(2), 1-6, 2019.
37. Vardhini, B., Dass, S. N., Sahana, R., & Chinnaiyan, R., "**A Blockchain based Electronic Medical Health Records Framework using Smart Contracts**". In 2021 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE, 2021.
38. Islam, N., Faheem, Y., Din, I. U., Talha, M., Guizani, M., & Khalil, M., "**A Blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services**". Future Generation Computer Systems, 100, 569-578, 2019.
39. Hussein, A. F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J. M. R., & de Albuquerque, V. H. C., "**A medical records managing and securing Blockchain based system supported by a genetic algorithm and discrete wavelet transform**". Cognitive Systems Research, 52, 1-11, 2018.
40. Chakraborty, S., Aich, S., & Kim, H. C., "**A secure healthcare system design framework using Blockchain technology**". In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 260-264). IEEE, 2019.
41. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A., "**Blockchain for secure EHRs sharing of mobile cloud based e-health systems**". IEEE access, 7, 66792-66806, 2019.
42. Bazel, M. A., Mohammed, F., & Ahmed, M., "**Blockchain Technology in Healthcare Big Data Management: Benefits, Applications and Challenges**". In 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA) (pp. 1-8). IEEE, 2021.
43. Huang, H., Sun, X., Xiao, F., Zhu, P., & Wang, W., "**Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments**". Journal of Parallel and Distributed Computing, 148, 46-57, 2021.
44. Cheng, X., Chen, F., Xie, D., Sun, H., & Huang, C., "**Design of a secure medical data sharing scheme based on Blockchain**". Journal of medical systems, 44(2), 1-11, 2020.

45. Alfaidi, A., & Chow, E., "**Health Record Chain (HRC): Implementation of Mobile Healthcare system using Blockchain to enhance Privacy of Electronic Health Record EHR**". In 2020 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 863-866). IEEE, 2020.
46. Jiang, S., Wu, H., & Wang, L., "**Patients-controlled secure and privacy-preserving EHRs sharing scheme based on consortium Blockchain**". In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE, 2019.
47. Mahdy, M. M., "**Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records**". In 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE) (pp. 1-4). IEEE, 2020.
48. Zhang, P., Schmidt, D. C., White, J., & Lenz, G., "**Blockchain technology use cases in healthcare**". In Advances in computers (Vol. 111, pp. 1-41). Elsevier, 2018.